THE EMERGING CONSENSUS ON CRIMINAL CONDUCT IN CYBERSPACE

BY

MARC D. GOODMAN AND SUSAN W. BRENNER

Article Outline

I. INTRODUCTION

II. WHAT IS CYBERCRIME AND WHY IS IT A SOURCE OF GLOBAL CONCERN?

A. WHAT IS CYBERCRIME?

1. *HACKING*
2. *VIRUSES AND OTHER MALICIOUS PROGRAMS*
3. *FRAUD AND THEFT*
4. *GAMBLING, PORNOGRAPHY AND OTHER OFFENSES AGAINST MORALITY*
5. *CHILD PORNOGRAPHY AND OTHER OFFENSES AGAINST MINORS*
6. *STALKING, HARASSMENT, HATE SPEECH*
7. *OTHER OFFENSES AGAINST PERSONS*
8. *CYBERTERRORISM*

B. "CRIME" VERSUS "CYBERCRIME"

C. INCIDENCE AND COSTS OF CYBERCRIME

III. WHAT MEASURES ARE BEING TAKEN TO COMBAT CYBERCRIME AT THE NATIONAL AND INTERNATIONAL LEVELS?

A. A BRIEF CHRONOLOGY: NATIONAL AND INTERNATIONAL EFFORTS

1. *THE ORIGINS OF COMPUTER CRIME AND NATIONAL LEGISLATION: 1960'S- 1970'S*
2. *THE MAIN WAVES OF NATIONAL LEGISLATION: 1970'S-1990'S*
3. *CHRONOLOGY OF INTERNATIONAL EFFORTS*
4. *CUMULATIVE BENEFITS*

B. CONSENSUS CRIMES: FOUNDATIONS OF A GLOBAL STRATEGY

1. *CONSENSUS CRIMES: WHAT ARE THEY?*

   a. CRIMES AGAINST PERSONS
   b. CRIMES AGAINST PROPERTY
   c. CRIMES AGAINST THE STATE
   d. CRIMES AGAINST MORALITY

2. *EFFORTS TO BUILD CONSENSUS*

   a. REVIEW OF EFFORTS TO BUILD CONSENSUS
   b. TWO PROPOSALS FOR THE ARTICULATION OF CONSENSUS CRIMES

      i. COUNCIL OF EUROPE CONVENTION
      ii. CISAC CONVENTION

   c. NOTE: THE LIMITS OF PENAL LAW CONSISTENCY

I. INTRODUCTION

> *Undeterred by the prospect of arrest or prosecution, cyber criminals around the world lurk on the Net as an omnipresent menace to the financial health of businesses, to the trust of their customers, and as an emerging threat to nations' security.*[1]

Nations around the world are very concerned about cybercrime, a concern shared by many international organizations, including the United Nations, the G-8, the European Union and the Council of Europe.[2] There are, as § II explains, a number of reasons to be concerned, perhaps the most important being the problems law enforcement officials and prosecutors encounter in trying to apply existing law cyberspace crime.

Many legal challenges faced by police and prosecutors in pursuit of cybercriminals can be illustrated by the brief yet destructive career of the "Love Bug" virus.[3] The virus destroyed files and stole passwords;[4] it appeared in Hong Kong on May 11, 2000 and spread rapidly throughout the world.[5]

> . . . .[I]n the offices of the German newspaper Abendblatt in Hamburg, system administrators watched in horror as the virus gobbled up 2,000 digital photographs in their picture archive. In Belgium ATMs were disabled, leaving citizens cashless. In Paris cosmetics maker L'Oréal shut down its e-mail servers, as did businesses throughout the Continent. As much as 70% of the computers in Germany, the Netherlands and Sweden were laid low. The companies affected made

---

[1] *Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information*, MCCONNELL INTERNATIONAL (December 2000), *at* http://www.mcconnellinternational.com/services/cybercrime.htm.

[2] *See* § III, *infra*.

[3] Technically, the "Love Bug" was both a virus and a worm:

> Fiendishly created, the Love Bug strikes with a one-two punch. Once you've clicked open that fatal attachment and activated its deadly code, the virus either erases or moves a wide range of data files. It singles out in particular so-called .jpgs and MP3s — digital pictures and music — and, like a natural virus, replaces them with identical copies of itself. Then, if it finds the Microsoft Outlook Express e-mail program on your computer, it raids the program's address book and sends copies of itself to everyone on that list. . . . Technically, this two-pronged approach makes the Love Bug both a virus and a worm; it's a virus because it breeds on a host computer's hard drive and a worm because it also reproduces over a network.

Lev Grossman, *Attack of the Love Bug*, TIME EUROPE, (May 15, 2000), *available at* http://www.time.com/time/europe/magazine/2000/0515/cover.html. For more on computer viruses and worms, *see, e.g.,* Jeffrey O. Kephart, et al., *Fighting Computer Viruses*, SCIENTIFIC AMERICAN, (Nov. 1997), *available at* http://www.sciam.com/1197issue/1197kephart.html; Bob Page, *A Report on the Internet Worm*, (Nov. 7, 1988), *at* ftp://coast.cs.purdue.edu/pub/doc/morris_worm/worm.paper; *Computer Abuse: Worms, Viruses, Trojan Horses*, *at* http://www.eos.ncsu.edu/eos/info/computer_ethics/abuse/wvt/.

[4] *See, e.g., Students Named in Love Bug Probe*, APBNEWS.COM, (May 20, 2000), *at* http://www.apbnews.com/newscenter/internetcrime/2000/05/10/lovebug0510_01.html; Rick Thomas, *Love Bug Virus Is No Herbie*, THE BUSINESS JOURNAL, (May 12, 2000), *available at* http://www.thepbj.com/051200/a19.htm.

[5] *See, e.g.,* Grossman, *supra* note 3.

> up a Who's Who of industry and finance, including Ford, Siemens, Silicon Graphics and Fidelity Investments. Even Microsoft . . . got so badly battered that it finally severed outside e-mail links at its Redmond, Wash., headquarters.
>
> Governments, too, felt the pain. In London, Parliament shut down its servers before the Love Bug's assault. . . .
>
> On Capitol Hill, crippled e-mail systems forced an atypical silence in the halls of Congress. . .
>
> The bug infected 80% of all federal agencies, including both the Defense and State departments, leaving them temporarily out of e-mail contact with their far-flung outposts. . . . [T]the virus corrupted no fewer than four classified, internal Defense Department e-mail systems. . . .[6]

The virus affected NASA and the CIA[7] on its two-hour race around the world , three times faster than its predecessor Melissa.[8] The virus is estimated to have ultimately affected over forty-five million users in more than twenty countries.[9] The various estimates of the damage caused, ranging from two billion dollars up to ten billion, reflect on the inherent difficulty of assessing the harm inflicted by cybercrime.[10]

Virus experts quickly traced the "Love Bug" to the Philippines.[11] Philippines' National Bureau of Investigation and United States FBI agents identified individuals suspected of creating and

---

[6] *Id.*

[7] *See, e.g., Experts Call for "Anti Love-Bug" Computer Czar*, APBNEWS.COM, (May 11, 2000), *at* http://www.apbnews.com/newscenter/internetcrime/2000/05/11/lovebug_congress0511_01.html.

[8] *See, e.g.,* Grossman, *supra* note 3.

[9] *See, e.g., Philippine Investigators Detain Man in Search for "Love Bug" Creator,* CNN.COM, (May 8, 2000), *at* http://www.cnn.com/2000/TECH/computing/05/08/ilove.you.02/; *Love Bug Suspect Suggests It Was "Accidental,"* apbnews.com (May 11, 2000), *at* http://www.apbnews.com/newscenter/internetcrime/2000/05/11/lovebug0511_01.html.

[10] *See* § II(C), *infra*. *See also* Colin Menzies, *Love Bug Was Just First Bite by a Very Dangerous Virus*, FINANCIAL REVIEW, (June 20, 2000), *at* http://afr.com/reports/20000620/A19850-2000Jun19.html:

> Want a worldwide damage estimate for the recent Love Bug virus? Try $US1 billion, or even $US10 billion. Or then again any figure between the two, because that's how wildly the estimates vary.
>
> The truth is no-one knows the real cost of the damage. As independent computer-industry analyst Graeme Philipson says: `The problem with any estimate of that nature is that it's impossible to quantify some of the effects. How do you quantify a professional's time if his hard disk has been scrubbed?
>
> `There's no physical cost, nothing breaks, there's no hardware damage ... it's all in people's time and lost data, which are notoriously unquantifiable figures.'

[11] *Id.*

disseminating the "Love Bug" using information supplied by an Internet Service Provider [12] but ran into problems with their investigation. Since the Philippines had no cybercrime laws, creating and disseminating the virus was not a crime; since there was no crime, the agents had a hard time convincing a magistrate to issue a warrant to search the suspects' apartment.[13] Getting the warrant took days, ample time to destroy evidence.[14] After finally executing the warrant authorities seized evidence indicating that Onel de Guzman, a former computer science student, was responsible for creating and disseminating the "Love Bug."[15] As hacking and the distribution of viruses had not been criminalized, officials struggled with whether de Guzman could be prosecuted. After finally charging him with theft and credit card fraud,[16] the watched the charges be dismissed as inapplicable and unfounded.[17] Because extradition

---

[12] *See, e.g., Caller ID Traced "Love Bug" Virus*, APBNEWS.COM, (May 15, 2000), *at* http://www.apbnews.com/newscenter/internetcrime/2000/05/15/lovebugid0515_01.html; *Philippine Investigators Detain Man in Search for "Love Bug" Creator*, *supra* note 9.

[13] *See, e.g.,* Lori Enos, *Police Nab Love Bug Suspect*, E-COMMERCE TIMES, (May 8, 2000), *at* http://www.ecommercetimes.com/perl/story/3247.htmlhttp://www.ecommercetimes.com/perl/story/3247.html; *Philippines' Laws Complicate Virus Case*, USA TODAY, (June 7, 2000), *available at* http://www.usatoday.com/life/cyber/tech/cth879.htm.

[14] *See Philippines' Laws Complicate Virus Case*, *supra* note 13 ("Federal agents were forced to delay a raid on an apartment where the virus is believed to have originated for days as prosecutors first searched for laws that could apply, then tried to persuade judges to issue a search warrant"). *See also Police Arrest "ILOVEYOU" Suspect*, ZDNET UK, (May 8, 2000), *at* http://news.zdnet.co.uk/story/0,,s2078816,00.html (Philippines official quoted as saying that the suspects could have erased computer evidence).

[15] *See, e.g., Waiting for "Love" Suspect*, ABCNEWS.COM, (May 8, 2000), *at* http://204.202.137.113/sections/tech/DailyNews/virus_000508.html (officers seized telephones, wires, computer disks and computer magazines from the de Guzman apartment). *See also Suspect Charged in Love Bug Case*, WIRED NEWS, (June 29, 2000), *at* http://www.wired.com/news/lovebug/0,1768,37322,00.html.

[16] The theory behind the charges was that the virus was designed to steal passwords which, in turn, would be fraudulently used to obtain Internet services and other things of value. *See, e.g.,"Love Bug" Suspect Not Off Hook Yet*, USA TODAY, (Sept. 5, 2000), *available at* http://www.usatoday.com/life/cyber/tech/cti482.htm.

[17] *See, e.g., Charges Dropped Against Love Bug Suspect*, USA TODAY, (Aug. 21, 2000), *available at* http://www.usatoday.com/life/cyber/tech/cti418.htm.

> Until President Joseph Estrada signed a new law in June covering electronic commerce and computer hacking, the Philippines had no laws specifically against computer crimes.
>
> The new legislation, however, cannot be applied retroactively to the "`love bug'' creator, and investigators instead charged de Guzman with traditional crimes such as theft and violation of a law that normally covers credit card fraud.
>
> The Department of Justice ruled that the credit card law does not apply to computer hacking and that investigators did not present adequate evidence to support the theft charge.
>
> The National Bureau of Investigation had waited more than a month to file the charges against de Guzman while it attempted to find applicable laws.
>
> 'Those are the only laws that our legal department has identified as being applicable,' Elfren Meneses, head of the NBI's anti-fraud and computer crimes division, said Monday. 'That's the best we have.'

treaties require "double criminality," that the act for which extradition is sought be a crime by the laws of each involved nation, de Guzman could not extradited for prosecution by other countries that do have cybercrime laws, such as the United States.[18] Despite having caused billions of dollars in damage to thousands of victims in numerous nations, de Guzman could not be brought to trial in the matter. So, no one was ever prosecuted for the damage the "Love Bug" caused.

Law enforcement officials cannot take action against cybercriminals unless countries first enact laws which criminalize the activities in which these offenders engage. As the "Love Bug" investigators learned, the existence of such laws is a fundamental prerequisite for investigation as well as for prosecution. It would therefore seem obvious that all nations would have or at least desire to have cybercrime laws on the books.

The difficulty lies in properly defining the laws needed to allow for cybercriminals' apprehension and prosecution. While seemingly a straightforward task, difficult issues are raised. One is whether the definitional scope of cybercrimes should include only laws that prohibit activities *targeting* computers or should outlaw crimes against individuals affected through the computer as well, such as cyberstalking and cyberterrorism. Another is whether these laws should be cybercrime-specific, targeting only crimes committed by exploiting computer technology. Is it, for example, necessary for a country to add a "computer fraud" offense if it has already outlawed fraud?

Both these issues are national in scope and go only to the nature of legislation a nation should adopt. Other issues are international in scope, pertaining to the impact a country's cybercrime laws, or lack thereof, have on other countries. The Philippines' failure to have cybercrime legislation meant that a Philippine national could not be tried in any of the twenty countries to which he inflicted damage and thus suffered no consequences for his acts; the failure to have legislation was inadvertent, but it's impact was felt around the globe. The "Love Bug" episode illustrates how fragile our modern networked world is: "[a]nyone with a computer and an Internet connection, no matter where, can use software easily available on the Web to spawn an electronic plague with global implications. 'There are no borders on the Internet.'"[19]

A recent study noted several ways in which cybercrimes differ from terrestrial crimes: "They are easy to learn how to commit; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present in it; and they are often not clearly illegal."[20] They also pose far greater challenges for law enforcement:

Id.

[18] *See, e.g.,* Lynn Burke, *Love Bug Case Dead in Manila*, WIRED NEWS (Aug. 21, 2000), *at* http://www.wired.com/news/print/0,1294,38342,00.html. *See also* Washington (State of) v. Johnson, [1988] 1 S.C.R. 327, *available at* http://www.lexum.umontreal.ca/csc-scc/en/pub/1988/vol1/html/1988scr1_0327.html.

[19] *Filipino Arrested in "Love Bug" Case*, ST. PETERSBURG TIMES ONLINE, (May 9, 2000), *at* http://www.sptimes.com/News/050900/Worldandnation/Filipino_arrested_in_.shtml. (quoting Robert Villabona, Operations Manager at Sky Internet, one of the internet service providers used to distribute the virus).

[20] *Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information, supra* note 1.

> [T]he laws of most countries do not clearly prohibit cyber crimes. Existing terrestrial laws against physical acts of trespass or breaking and entering often do not cover their `virtual' counterparts. Web pages such as the e-commerce sites recently hit by widespread, distributed denial of service attacks may not be covered by outdated laws as protected forms of property. New kinds of crimes

> Effective law enforcement is complicated by the transnational nature of cyberspace. Mechanisms of cooperation across national borders to solve and prosecute crimes are complex and slow. Cyber criminals can defy the conventional jurisdictional realms of sovereign nations, originating an attack from almost any computer in the world, passing it across multiple national boundaries, or designing attacks that appear to be originating from foreign sources. Such techniques dramatically increase both the technical and legal complexities of investigating and prosecuting cyber crimes.[21]

Nations must modernize their procedural law as well as their substantive law, their law of crimes. While an adequate framework of cybercrime penal law is an absolute prerequisite for effective action against cybercriminals, such action can be frustrated by antiquated procedural law which, for example, authorizes warrants only for search for and seizure of tangible evidence.[22] Since the prosecution of cybercrimes usually requires collecting and analyzing intangible evidence, this omission can be a serious problem for investigators.[23] Countries must, therefore, also evaluate their procedural law governing evidence collection and analysis, and amend existing legislation as necessary so as to not suffer from such limitations.[24]

> can fall between the cracks, as the Philippines learned when it attempted to prosecute the perpetrator of the May 2000 Love Bug virus. . . .

Id.

[21] *Id.*

[22] *See, e.g.,* D.C. SUPER. CT. RULES CRIM. PRO. 41(h) ("The term 'property' is used in this rule to include documents, books, papers and any other tangible objects"). *Accord* MAINE R. CRIM. PRO. 41(g).

[23] *See, e.g.,* Explanatory Report, Council of Europe, Convention on Cybercrime, ¶ 171 (November 8, 2001), http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm:

> [T]here are some differences with respect to the search of computer data, which may necessitate different or special procedural provisions to ensure that computer data can be obtained in a manner that is equally effective as a search and seizure of tangible data. First, the data is in intangible form, such as in an electromagnetic form. Second, while the data may be read with the use of computer equipment, it cannot be seized and taken away in the same sense as can a paper record. The physical medium on which the intangible data is stored (e.g., the computer hard-drive or a diskette) must be seized and taken away, or a copy of the data must be made in either tangible form (e.g., computer print-out) or intangible form on a physical medium (e.g., diskette), and the tangible medium containing the copy is seized and taken away. In the latter two situations where copies of the data are made, the original data remains in the computer system or storage device. Some changes may be required to domestic law to ensure that intangible data can be searched and seized. Third, due to the connectivity of computer systems, data may not be stored in the particular computer that is searched, but such data may be readily accessible to that system. It could be stored in an associated data storage device that is connected directly to the computer, or connected to the computer indirectly through communication systems, such as the Internet. This may or may not require new laws to permit an extension of the search to where the data is actually stored (or the retrieval of the data from that site to the computer being searched), or the use traditional search powers in a more co-ordinated and expeditious manner at both locations.

[24] *See, e.g.,* Model Code of Cybercrime Investigative Procedure, Article VII, *at* http://www.cybercrimes.net/MCCIP/art7.htm.

To prevent the recurrence of another "Love Bug" scenario, the Philippines quickly adopted legislation outlawing certain types of cybercrimes, including the creation and dissemination of viruses.[25] But since legislation is a product of a nation's political and social philosophies, countries may not agree as to what should be defined as a cybercrime. Some countries, for example, make it a crime to publish "hate speech" or otherwise incite "racial hatred."[26] In the United States, such activity is protected by the First Amendment, which creates a conflict of cybercrime law.[27]

These issues are the focus of this article; it examines how they are being addressed at the national and international levels and assesses the measures that are being taken in an effort to resolve them. Section II provides a context for the discussion; it compares "cybercrime" with "terrestrial crime" and explains why the former has become a national and international concern. Section III reviews the state of cybercrime legislation around the world; it also introduces the concept of "consensus crimes" and explains how this concept can be used to achieve an essential level of consistency in global cybercrime legislation. Also examined in Section III are other strategies nations can, and should employ in their battles against cybercrime. Finally, Section IV provides a brief conclusion, summarizing the points made in the earlier sections and offering some final reflections on these issues.

II. WHAT IS CYBERCRIME AND WHY IS IT A SOURCE OF GLOBAL CONCERN?

Unlike traditional crime, cybercrime is global crime.[28] As a European Commission report explains, "[c]omputer-related crimes are committed across cyber space and do not stop at the conventional state-borders. They can . . . be perpetrated from anywhere and against any computer user in the world."[29]

---

[25] *See, e.g., "Love bug" Prompts New Philippine Law*, USAToday (June 14, 2000), *available at* http://www.usatoday.com/life/cyber/tech/cti095.htm (under the new law, hackers and those who spread computer viruses can be fined a minimum of $2,350 and a maximum "commensurate" with the damage caused, and can be imprisoned for up to three years). *See also* Republic of the Philippines, Eleventh Congress – Second Regular Session, Republic Act No. 8792, Part V § 33, *available at* http://www.mcconnellinternational.com/services/country/philippines.pdf.

[26] *See, e.g.,* Elizabeth G. Olson, *Nations Struggle with How to Control Hate on the Web*, N.Y. TIMES, (Nov. 24, 1997), *available at* http://www.nytimes.com/library/cyber/week/112497racism.html. *See also* Dave Amis, *The Net Now Has a National Court: This Month It's French!*, INTERNET FREEDOM NEWS, (Jan. 9, 2001), *at* http://www.netfreedom.org/news.asp?item=137 (French law prohibits sale of material inciting racial hatred).

[27] *See, e.g., Seminar on the Role of Internet with regard to the Provisions of the International Convention on the Elimination of All Forms of Racial Discrimination*, Item V (Prohibition of Racist Propaganda on the Internet Juridicial Aspects, International Measures), U.N. HIGH COMMISSIONER FOR HUMAN RIGHTS, (Nov. 10-14, 1997), *at* http://www.unhchr.ch/html/menu2/10/c/racism/shahi.htm:

> In the United States, anti-semitic and racist speech on the Internet is protected by the First Amendment guarantee of freedom of expression. Consequently, material that is treated as illegal in most other democracies outside the US, including racist and defamatory statements, will be presented on the Internet (via US postings) and as a result, would be accessible to virtually everyone around the globe, regardless of existing local laws and mores.

[28] *See* § II(B), *infra*.

[29] *Communication from the European Commission to the Council and the European Parliament, Creating a Safer Information Society By Improving the Security of Information Infrastrutures and Combating Computer-Related*

Technology gives the ability to loot and inflict harm upon the entire world with little risk of apprehension[30] and allows for experimenting with new varieties of criminal endeavors.[31] The sections below examine the distinct phenomenon of "cybercrime," [32] compare it with traditional crime[33] and review the statistics that have been compiled on its incidence and the damage it inflicts. [34]

A. WHAT IS CYBERCRIME?

The terms "cybercrime," "computer crime", "Information Technology crime," and "high-tech crime" are often used inter-changeably to refer to two major categories of offenses: in the first, the computer is the target of the offense; attacks on network confidentiality, integrity and/or availability -- i.e. unauthorized access to and illicit tampering with systems, programs or data – all fall into this category;[35]

Crime 9 (2000), *available at* http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeCommEN.html [hereinafter *Creating a Safer Information Society*].

[30] *See, e.g., Conclusions of the Study on Effective Measures to Prevent and Control High-Technology and Computer-Related Crime*: *Report of the Secretary-General*, U.N. Commission on Crime Prevention and Criminal Justice, 10th Sess., Item 4 at 12, U.N. Doc. E/CN.15/2201/4 (2001), *available at* http://www.odccp.org/adhoc/crime/10_commission/4e.pdf:

> [t]he specific qualities of the Internet may induce a perpetrator to use it instead of traditional means; it offers excellent communication facilities and the possibility of hiding one's identity, and the risk of being subjected to criminal investigation, in any of the jurisdictions involved, is relatively low .

[31] *See, e.g., Crimes Related to Computer Networks*, Tenth United Nations Conference on the Prevention of Crime and the Treatment of Offenders, Vienna, 10-17 Apr., 2000, A/CONF.187/10, at 5:

> the international character of modern computer and telecommunications technologies has led to new forms of transnational and multinational crime. The concept of cyberspace and the ease with which criminal acts in one geographic location can have effects in others makes the integration of national and international measures essential. Without such integration, counter-measures may be ineffective against crime. . . .

See also Conclusions of the Study on Effective Measures to Prevent and Control High-Technology and Computer-Related Crime, *supra* note 30:

> [t]he specific qualities of the Internet may induce a perpetrator to use it
>
> instead of traditional means: it offers excellent communication facilities and the possibility of hiding one's identity, and the risk of being subjected to criminal investigation, in any of the jurisdictions involved, is relatively low .

[32] *See* § II(A), *infra*.

[33] *See* § II(B), *infra*.

[34] *See* § II(C), *infra*.

[35] *See* Marc D. Goodman, *Why the Police Don't Care About Computer Crime*, 10 HARV. J.L. & TECH., 465, 468-469 (1997), *available at* http://jolt.law.harvard.edu/articles/10hjolt465.html. *See also Criminal Threats to E-Commerce* 17, INTERPOL, Jan. 2001.

the other category consists of traditional offenses -- such as theft, fraud, and forgery – that are committed with the assistance of or by means of computers, computer networks and related information and communications technology.[36] This article uses the broad definition of "cybercrime," referring to offenses falling into either category.

Computers can also play an incidental role in the commission of a traditional offense, as when a blackmailer uses a computer to generate blackmail letters (or e-mails) or a drug dealer who uses Quicken to track his drug purchases and sales.[37] This article will not specifically address such instances ; because the computer plays such a peripheral role in these scenarios, they are unlikely to require adoption of new substantive cybercrime law to allow the apprehension and prosecution of the perpetrator. This is not to say that they pose no challenges for law enforcement; like the "true" cybercrime brethren, they will contribute to an enormous amount of cyber-forensic work which will soon become a routine part of criminal investigations, for which law enforcement is wholly unprepared.[38]

Cybercrimes range from economic offenses (fraud, theft, industrial espionage, sabotage and extortion, product piracy, etc.) to infringements on privacy, propagation of illegal and harmful content, facilitation of prostitution and other moral offenses , and organized crime.[39] At its most severe, cybercrime borders on terrorism, encompassing attacks against human life and against national security establishments, critical infrastructure, and other vital veins of society. Terrorism encompasses actions

---

[36] *Id*.

[37] Goodman, *supra* note 35.

[38] *See Criminal Threats to E-Commerce*, *supra* note 35, at 26:

> The investigative techniques used to solve and investigate many crimes are the same: identify the victim, locate physical evidence, determine the identity of the perpetrator, and arrest him. In the case of a commercial burglary, this is a relatively simple matter. The victim will almost always phone the police, who will go to the scene of the crime. All officers are trained to conduct burglary investigations: the police will look for a point and method of entry, and attempt to determine what items were taken in the crime. The police collect any physical evidence such as fingerprints or tools used to pry open a window and send to a laboratory for analysis.
>
> Of course, the same sort of burglary could be committed `virtually' with a computer. The thief would break into a computer system, steal computer files, and transport the stolen items back to his own machine. . . . [T]he methods and means of proceeding are not so clear. Unlike a real world burglary in which the victim returns home to find a television obviously missing, a virtual burglary need only copy the property he covets, leaving the original behind. Thus the victim of a cybertheft may have no idea that any of his computer files have been stolen.
>
> . . . . Even if a computer crime victim realised an intrusion had taken place, he might be afraid to report the matter to the authorities, fearing the loss of his customers' confidence. Furthermore, in the non-corporeal world locating physical evidence is no easy task: police officers are used to having evidence they can see and feel such as screwdrivers, knives, and handguns. Digital evidence is something altogether different. Even if officers were attuned to its presence, how would they physically take it into custody? How would they remove the evidence from the computer, process it, and prepare it for presentation in court? Most police agencies are vastly under-prepared for this type of investigation.

[39] *See, e.g., Criminal Threats to E-Commerce*, *supra* note 35, at 17.

intended to provoke a state of terror in the general public, a group of persons or particular persons.[40] Terrorist acts cause grave harm to society by disrupting civil order and/or causing mass terror, loss of life, physical destruction or economic hardship.[41] In cyberterrorism, as in cybercrime, the "cyber" component usually refers to perpetrating qualitatively new offenses enabled by information technology or integrating cyberspace into more traditional activities (such as planning, intelligence, logistical capabilities, finance, etc.).[42] The categories may also overlap, as they frequently do in the cases of capable, computer-savvy offenders.

As this survey demonstrates, cybercrimes are complex and sometimes elusive phenomena; there is no comprehensive, globally accepted definition that separates the sensational from the sensible and scientific. The following scenarios -- all quite real and frequent occurrences --illustrate the range of activities that can be considered cybercrimes.

1. HACKING AND RELATED ACTIVITIES

Hacking, or gaining unauthorized access to a computer system, programs or data, opens a broad playing field for inflicting damage. A snooper might read the victim's personal information and even take over his computer,[43] or a vandal might alter the victim's webpage.[44] A saboteur could erase R&D data or

---

[40] *Threat of Terrorism in the United States*, *Statement before the Senate Committee on Appropriations, Armed Services and Select Committee on Intelligence*, 107th Congress. (May 10, 2001) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation) *available at* http://www.fbi.gov/congress/congress01/freeh051001.htm:

> International terrorism involves violent acts, or acts dangerous to human life, that are a violation of the criminal laws of the United States or any state, or that would be a criminal violation if committed within the jurisdiction of the United States or any state, and which are intended to intimidate or coerce a civilian population, influence the police of a government, or affect the conduct of a government. Acts of international terrorism transcend national boundaries in terms of the means by which they are accomplished, the intended persons they appear to intimidate, or the locale in which the perpetrators operate.

See also 22 U.S.C. § 2656f(d) ("terrorism" means premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience).

[41] *See, e.g.,* REPORT OF THE NATIONAL COMMISSON ON TERRORISM, COUNTERING THE CHANGING THREAT OF INTERNATIONAL TERRORISM § 1 (June 7, 2000), *at* http://www.terrorism.com/documents/bremercommission/index.shtml.

[42] *See, e.g.,* Dorothy E. Denning, *Cyberterrorism: Testimony Before the Special Oversight Panel on Terrorism, House Committee on Armed Services,* (May 23, 2000), *at* http://www.terrorism.com/documents/denning-testimony.shtml.

[43] *See, e.g.,* Nicky Blackburn, *Forget Viruses, The Trojans Are Coming*, THE JERUSALEM POST, (June 4, 2000), *at* http://www.jpost.com/Editions/2000/05/28/Digital/Digital.7384.html:

> A user may receive an innocent looking e-mail, but embedded within the attachment, or in some cases even the HTML message itself, is a coded page which connects your PC to a Web site. From there a small trojan horse . . . is downloaded into your computer and the hacker . . . is alerted . . . that the computer has been penetrated.

paralyze a network, and an industrial spy might steal trade secrets.[45] A blackmailer might plant a digital time/logic bomb and threaten to trash a system unless the victim pays up.[46]

2. VIRUSES AND OTHER MALICIOUS PROGRAMS

Section I describes the damage done by the "Love Bug," a virus that may have been unleashed unintentionally. Other viruses and other types of malicious code can be even more destructive: A calamitous virus may delete files or permanently damage systems. A Trojan horse, masquerading as a utility (e.g. anti-virus software) or animation, may copy user-IDs and passwords, erase files, or release viruses. The program may be used for blackmail, with activation of a virus or 'detonation' of a digital bomb threatened unless demands are met. A virus might cause a minor annoyance, or tremendous losses in money and productivity, or even human lives, if it changes or destroys crucial data such as hospital medical records.[47]

3. FRAUD AND THEFT

Fraud represents what is probably the largest category of cybercrime:

> The hacker can then add however many programs he wants to the victim's computer, allowing him access to the most personal files, be they financial plans or letters to a lover. In some circumstances the hacker can even have remote control of the computer itself, a threat with many worrying implications.

[44] *See, e.g., Hackers Deface Army's Web Site*, APBNEWS.COM, (June 28, 1999), *at* http://www.apbnews.com/newscenter/breakingnews/1999/06/28/hack0628_01.html.

[45] *See, e.g.,* Melvin F. Jager & William J. Cook, *Trade Secrets & Industrial Espionage – Online Piracy*, BHG&L RESOURCES 1996, *at* http://www.brinkshofer.com/resources/tradesecrets.cfm:

> Eugene Wang allegedly used his MCI E-mail account at Borland to transfer Borland trade secrets to his future employer, Gordon Eubanks at Symantec. This material included Borland's product design specifications, product development strategies, sales data, and information regarding a prospective contract for which both companies were competing.

[46] *See, e.g.,* Steven Lohr, *A New Battlefield: Rethinking Warfare in the Computer Age*, N.Y. TIMES, (Sept, 30, 1996), *available at* http://is.gseis.ucla.edu/impact/f96/Projects/smistry/nytwar.html:

> Private investigators and bankers say they are aware of four banks, three in Europe and one in New York, that have made recent payments of roughly $100,000 each to hacker extortionists. The bankers and investigators would not name the banks, but the weapon used to blackmail the banks was a logic bomb -- a software program that, when detonated, could cripple a bank's internal computer system. In each case, the sources said, the banks paid the money, and then took new security measures.

[47] Louis J. Freeh, Director, Federal Bureau of Investigation, *Statement Before the Senate Committee for the Judiciary – Subcommittee on Technology, Terrorism and Government Information*, (Mar. 28, 2000), *available at* http://www.usdoj.gov/criminal/cybercrime/freeh328.htm.

> The Internet has . . . created what so far appears to be the perfect cybercrime—borderless fraud. So many different types of fraud are committed over computer networks that they have become almost impossible to police effectively. In computer chat-rooms, message boards, unsolicited e-mail, and on web sites themselves, fraudsters lose no opportunity to trick and deceive others for the purpose of financial gain.
>
> Those who engage in fraud operate globally on `Internet time,' 24 hours a day, 7 days a week. . . . Although many of the schemes perpetrated online today are nothing more than repackaged versions of their `real world' counterparts, the efficiency and speed of the network create new opportunities for criminals while simultaneously positing serious criminal threats to e-commerce.[48]

One of the most common types of cyberfraud is online auction fraud:[49] You are buying something you saw advertised on eBay, for example. Is the person you are dealing with trustworthy? Often not: the vendor may be describing products or services in a false or misleading manner, or may take orders and money, but fail to deliver goods.[50] Counterfeit goods might be supplied. [51] Investment fraud has been seen, whereby the Internet is used to fraudulently manipulate stock prices or facilitate illegal insider trading. [52]

Using computers, thieves can steal credit card details[53] and siphon funds from banks.[54] A twenty-five year old Moscow hacker stole credit card information that was put onto blank cards and used at

---

[48] *Criminal Threats to E-Commerce*, *supra* note 35, at 26.

[49] *Id.* at 54.

[50] *Id.* at 54-56.

[51] *Id.*

[52] *See, e.g.,* Freeh, *supra* note 47:

> On April 7, 1999, visitors to an online financial news message board operated by Yahoo!, Inc. got a scoop on PairGain, a telecommunications company based in Tustin, California. An e-mail posted on the message board under the subject line `Buyout News' said that PairGain was being taken over by an Israeli company. The e-mail also provided a link to what appeared to be a website of Bloomberg News Service, containing a detailed story on the takeover. As news of the takeover spread, the company's publicly traded stock shot up more than 30 percent, and the trading volume grew to nearly seven times its norm. There was only one problem: the story was false, and the website on which it appeared was not Bloomberg's site, but a counterfeit site. When news of the hoax spread, the price of the stock dropped sharply, causing significant financial losses to many investors who purchased the stock at artificially inflated prices. . . .
>
> . . . [N]ineteen people were charged in a multimillion-dollar New York-based inside trading scheme. . . . [T]he Internet took a starring role as allegedly about $8.4 million was illegally pocketed from secrets traded in cyberspace chat rooms. . . . [A] disgruntled part-time computer graphics worker allegedly went online and found other disgruntled investors of the company in America Online chat rooms. He soon was passing inside information on clients of Goldman Sachs and Credit Suisse First Boston to two other individuals in exchange for a percentage of any profits they earned by acting on it. For 2-1/2 years, this employee passed inside information, communicating almost solely through online chats and instant messages. The part-time computer graphics worker received $170,000 in kickbacks while his partners made $500,000.

[53] *See id.*:

ATMs all over Europe; the fifty people involved in the scam managed to steal several million dollars before they were caught. [55]

Cyberspace can be just as easily used to commit theft-by-threat or extortion, as one company learned last year:

> [A] 19-year old Russian student using the name `Maxim' stole 300,000 credit card numbers from the computer server of CD Universe. Maxim extorted CD Universe by agreeing to destroy the customer data he had stolen in exchange for $100,000 cash. CD Universe did not pay the thief quickly enough for his liking, and Maxim published the credit card and customer data of 25,000 victims online. The event was widely re ported in the media and was quite damaging to CD Universe's reputation. . . .Maxim still remains at large.[56]

4. GAMBLING, PORNOGRAPHY AND OTHER OFFENSES AGAINST MORALITY

Online casinos have proliferated widely,[57] despite that fact that gambling is illegal in many jurisdictions.[58] The Internet is also being used to distribute drugs, tobacco and liquor, again regardless of jurisdictional prohibitions.[59]

5. CHILD PORNOGRAPHY AND OTHER OFFENSES AGAINST MINORS

Many types of pedophilic activity - viewing images, discussing activities, arranging tourism, enticing a child to a meeting - are carried out over the Internet.[60] As one report explained:

> [A]uthorities in Wales . . . arrested two individuals for . . . the theft of credit card information on over 26,000 accounts. One subject used the Internet alias 'CURADOR.' Losses from this case could exceed $3,000,000.

[54] In 1994, Russian hacker Vladimir Levin and his accomplices transferred $12 million out of Citibank accounts and into foreign accounts under their control. *See, e.g., Hacker Goes to Jail After Foiled Citibank Fraud Attempt*, INFOWAR.COM, (Feb. 26, 1998), *at* http://www.infowar.com/HACKER/hack_030198s_e.html-ssi.

[55] Arnaud de Borchgrave, et al., *Cyber Threats and Information Security: Meeting The 21st Century Challenge,* v, Center for Strategic and International Studies (2000), *at* http://www.csis.org/pubs/2001_cyberthreatsandis.htm.

[56] *Criminal Threats to E-Commerce*, *supra* note 35, at 57.

[57] According to one estimate, there are "approximately 200+ casinos, sportsbooks, and full service venues operating on the internet." *A Personal Message*, ONLINE CASINO GAMBLING, *at* http://www.adult-fun.net.

[58] *See, e.g.,* Tom W. Bell, *Policy Analysis*, ANTEUP GAMBLING LINKS, *at* http://gamblinglinks.com/legal.html (legality of online gambling in several jurisdictions).

[59] *See, e.g.,* Liquor Online, http://www.abaloneweb.com/stores/Liquor&Spirits/liquoronline.html-ssi; Cigarts.com, http://www.cigarts.com/; Mexico Pharmacy Online, http://www.mexico-pharmacy-online.com/mex-phar/mex-phar.htm.

[60] *See, e.g.,* INTERNET WATCH FOUNDATION, http://www.internetwatch.org.uk/; Movement Against Pedophilia on Internet, http://www.info.fundp.ac.be/~mapi/mapi-eng.html. *See also Tourism and Child Abuse: The Challenges to Media and Industry*, INTERNATINAL FEDERATION OF JOURNALISTS, *available at* http://www.ifj.org/working/issues/children/sextourism.html.

> Child sexual abusers are rapidly turning the Internet and commercial online services into red-light districts, where they can distribute vast quantities of pornography — often depicting bondage and other forms of violence, including murder — and organize with like-minded individuals. The Internet gives child molesters and pornographers unprecedented opportunities to target and recruit new victims. It allows sexual predators to stalk juvenile victims anonymously from the comfort of their homes.[61]

The Internet gives the pedophile the advantages of a wider scope of communications and the likelihood of eluding the law, given the jurisdictional problems which arise in prosecuting cases that transcend borders, as is the nature of the Internet.[62]

6. STALKING, HARASSMENT, HATE SPEECH

Stalking and harassment are malicious activities directed at a particular person, as two notorious California cases illustrate:

> [A] 50-year-old former security guard . . . used the Internet to solicit the rape of a woman who rejected his romantic advances. . . .[He] terrorized his 28-year-old victim by impersonating her in various Internet chat rooms and online bulletin boards, where he posted, along with her telephone number and address, messages that she fantasized of being raped. On at least six occasions, sometimes in the middle of the night, men knocked on the woman's door saying they wanted to rape her. . . .
>
> An honors graduate from the University of San Diego terrorized five female university students over the Internet for more than a year. The victims received hundreds of violent and threatening e-mails, sometimes receiving four or five messages a day. The graduate student . . . told police he committed the crimes because he thought the women were laughing at him and causing others to ridicule him. In fact, the victims had never met him.[63]

The dissemination of hate and racist speech has a more general focus,[64] but can be equally traumatic for those it targets, and is becoming more widespread, thanks to the Internet.[65]

---

[61] NEW JERSEY ATTORNEY GENERAL & COMMISSION OF INVESTIGATION, COMPUTER CRIME: A JOINT REPORT 6 (June 2000).

[62] *See, e.g.,* Opening Address by Ron O'Grady, Interpol: Child Pornography on the Internet Experts Meeting, Lyon, France, (May 28-29, 1998), *at* http://www.ecpat.net/Childporn/Ron's.html.

[63] U.S. Department of Justice, *Cyberstalking: A New Challenge for Law Enforcement and Industry*, (Aug. 1999), *at* http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm.

[64] *See, e.g.,* Rights for Whites Web Ring, http://nav.webring.yahoo.com/hub?ring=whitering&list; Vlaams Blok, http://www.vlaams-blok.be/; Holocaust Denial, http://www.okneoac.com/dtsantijew.html.

[65] *See, e.g.,* NEW JERSEY ATTORNEY GENERAL & COMMISSION OF INVESTIGATION, COMPUTER CRIME: A JOINT REPORT, *supra* note 61, at 32,34:

> Cyberspace permits hate mongers, bigots, racists . . ., Holocaust deniers, . . . anti-Semites and immigrant bashers to reach vast new audiences of potential adherents. . . .

> The e-mail address of a group of Jewish students in Germany was bombarded with more than 17,000 messages from adolf@hitler.com containing a threat to repeat the Holocaust. The murder of six million more Jews, the sender threatened, would start Nov. 9 - the anniversary of Kristallnacht, the Nov. 9, 1938 'Night of Broken Glass' when the Nazi regime orchestrated attacks on Jews and Jewish businesses across Germany in a harbinger of the Holocaust. German cyber police conceded they were powerless to investigate because the e-mails were sent via a server in the U.S., material that falls outside German laws that make neo-Nazi propaganda a crime. Germany has repeatedly complained that U.S. free speech laws have crippled its efforts to stop the spread of Neo-Nazi ideas via the Internet.[66]

Stalking, harassment, hate-filled and racist speech perpetrated over computer networks may or may not be criminal activities, depending on the jurisdiction.[67]

7. Other Offenses Against Persons

Cyberhomicide--using computer technology to kill someone--has not yet been reported, but it no doubt will. An aspiring mass murderer could, for example, hack into a hospital's computer system, learn about the medication prescribed for patients and alter the dosages, causing them to die.[68]

> The Internet facilitates mass dissemination of slick propaganda via Web sites accessible to millions. . . . [I]t creates a `virtual community' of like-minded believers. . . .

[66] Borchgrave, *supra* note 55, at i.

[67] *See, e.g.,* New Jersey Attorney General & Commission of Investigation, *supra* note 61:

> On September 20, 1996, a student who had flunked out of the University of California at Irvine (UCI) sent an anonymous, profanity-laced message to 59 Asian students. The message told them that if they did not 'get the ____ out of UCI,' he would 'hunt all of you down and Kill your stupid asses.' The message continued, 'I personally will make it my life career to find and kill everyone of you personally.'
> An administrator at the computer lab quickly collared the former student, who carelessly included his own name . . . on the list of recipients. . . . Local police declined to prosecute, but the FBI heard about the case and it became the first federal prosecution of a hate crime in cyberspace to go to trial.
>
> The former student was prosecuted under an obscure 1960s civil-rights Statute. . . .The law seeks to punish anyone who `by force or threat of force attempts to injure, intimidate or interfere with … any person because of his race, color or national origin and because he is or has been enrolling in or attending any public school or public college.' The jury convicted the former student of one of two counts, and the judge sentenced him to a year in prison.

The Machado Case, INTERNET FREEDOM, http://www.netfreedom.org/racism/material.html.

[68] *See, e.g.,* Freeh, *supra* note 47:

> In . . . 1999 the National Library of Medicine (NLM) computer system, relied on by hundreds of thousands of doctors and medical professionals from around the world for the latest information on diseases, treatments, drugs, and dosage units, suffered a series of intrusions where system administrator passwords were obtained, hundreds of files were downloaded which included sensitive medical 'alert' files and

Cyberspace can be used to commit extortion, as one company learned last year:

> [A] 19-year old Russian student using the name `Maxim' stole 300,000 credit card numbers from the computer server of CD Universe. Maxim extorted CD Universe by agreeing to destroy the customer data he had stolen in exchange for $100,000 cash. CD Universe did not pay the thief quickly enough for his liking, and Maxim published the credit card and customer data of 25,000 victims online. The event was widely re ported in the media and was quite damaging to CD Universe's reputation. . . .Maxim still remains at large.[69]

8. CYBERTERRORISM

Cyberterrorism has been defined as a "premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by subnational groups or clandestine agents."[70] Such an attack can take many forms:[71] a cyberterrorist might hack into computer systems and disrupt domestic banking, the stock exchanges and international financial transactions, leading to a loss of confidence in the economy. Or he might break into an air traffic control system and manipulate it, causing planes to crash or collide. A terrorist could hack into a pharmaceutical company's computers, changing the formula of some essential medication and causing thousands to die. Or a terrorist could break into a utility company's computers, changing pressure in gas lines, tinkering with valves and causing a suburb to detonate and burn.[72]

B. "TERRESTRIAL CRIME" VERSUS "CYBERCRIME"

Historically, "crime" was addressed at the local, community level of government.[73] Until the last century, crime was small-scale, consisting of unlawful acts committed by one person or a few loosely-

---

> programming files that kept the system running properly. The intrusions were a significant threat to public safety and resulted in a monetary loss in excess of $25,000. . . .

See also 1999 Revision of the Model State Computer Crimes Code, Commentary to § 2.01.1, http://www.cybercrimes.net/99MSCCC/MSCCC/Article2/2.01.1.html (committing mass murder by hacking into an industry computer and altering a product, such as an automobile, so that the product ultimately fails and kills its users).

[69] *Criminal Threats to E-Commerce*, *supra* note 35, at 57.

[70] Mark M. Pollitt, "*Cyberterrorism--Fact or Fancy?",* Proceedings of the 20th National Information Systems Security Conference, 285, October 1997 (quoted in Dorothy E. Denning, *Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*), *at* http://www.nautilus.org/info-policy/workshop/papers/denning.html.

[71] *See, e.g.,* John Arquilla, *The Great Cyberwar of 2002*, WIRED, (Feb. 1998), *at* http://www.wired.com/wired/archive/6.02/cyberwar_pr.html.

[72] *See, e.g., CyberWar*, RESEARCH-PAPERS.COM, *at* http://www.research-papers.com/papers/tech2.shtml.

[73] *See, e.g. The History of Policing*, ENCYCLOPAEDIA BRITANNICA, http://208.154.71.60/bcom/eb/article/2/0,5716,115162+1+108569,00.html; *A Brief History of Law Enforcement*, *at* http://hometown.aol.com/mre2all/A_Little_Historyindex.html.

associated persons that were directed against a single victim. Some offenders, of course, made crime their profession, but their activities remained small-scale, limited to the repetitive commission of certain single-victim offenses. The "crimes," which were generally consistent across societies, fell into standard, clearly-defined categories that reflected the basic categories of anti-social motivations: crime was murder, robbery and rape.[74] Crime also tended to be personal; if the offender(s) and victim did not actually know each other, they were likely to share community ties that put offenses into a manageable, knowable context. This not only facilitated the process of apprehending offenders—who stood a good chance of being identified by the victim or by reputation—it also gave citizens at least the illusion of security, the conceit that they could avoid being victimized if they avoided certain activities or certain associations. Local law enforcement dealt effectively with this type of crime because its parochial character meant investigations were limited in scope and because the incidence of crime stood in relatively modest proportion to the size of the local populace. Law enforcement's effectiveness in this regard contributed to a popular perception that social order was being maintained and that crime did not go unsolved or unpunished.

The twentieth century's increased urbanization, geographical mobility and use of technology undermined this model to some extent, but it persisted and still functioned effectively for the most part. Legal systems quickly adapted to the fact that telephones could be used to commit fraud and to harass others; that motor vehicles introduced a dimension of mobility into robbery, kidnapping and other crimes;[75] and that radio and television could be used to perpetrate crimes. Because legal systems modified their substantive criminal law to encompass these activities, the old model still functions effectively for traditional, "real world" crime. Cybercrime is a different story:

> Computers and the Internet have created phenomenal possibilities for addressing a variety of human problems, but . . . these technologies also have a dark side.

---

[74] *See, e.g.,* SIR WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND, BOOK IV: OF PUBLIC WRONGS (1769).

[75] *See, e.g.,* Kathleen F. Brickey, *Criminal Mischief: The Federalization of American Criminal Law*, 46 HASTINGS L.J. 1135, 1142-1144 (1995):

> The first part of the twentieth century brought with it the Mann Act (prohibiting transporting a woman across state lines for illicit purposes), the Dyer Act (prohibiting transporting a stolen motor vehicle across state lines), . . . and statutes forbidding interstate transportation of lottery tickets, interstate transportation of obscene literature, and selling liquor through the mail. . . . Congress had begun to rely on the commerce power . . . to enlarge federal criminal jurisdiction. The advent of railroads, automobiles**,** and airplanes made state boundaries `increasingly porous.' . . .
>
> By the 1930s the federalization of American criminal law was in full swing. During this era Congress enacted the Lindbergh Act (prohibiting the transportation of a kidnapping victim across state lines), the Fugitive Felon Act (prohibiting interstate flight to avoid prosecution for enumerated violent felonies), the National Firearms Act (regulating the sale of guns), the National Stolen Property Act (prohibiting the transportation of stolen property in interstate commerce), and statutes that punished . . . extortion by telephone, telegraph or radio, and much more.
>
> These developments were critical because they transformed what had been uniquely local concerns into national ones. Because `twentieth century criminals had wheels and wings, 'crime was now perceived as an interstate problem beyond the power of states to effectively address.

Id. (footnotes omitted).

> What differentiates the criminal threats posed by the Internet is that it is based on a vastly more complex technology than the automobile. It spans the globe and moves information and potential criminal activity with a speed and efficiency heretofore unknown in human history. Not only does this give the police less time to react to any potential criminal threat, but it raises issues of jurisdiction, privacy, and anonymity.[76]

Some cybercrimes such as stalking tend to be small-scale, single-offender/single-victim crimes. Although our experience with cybercrime is still in its infancy, large-scale offenses targeting multiple, geographically dispersed victims have already been committed. The February, 2000 denial of service attacks that targeted eBay, Yahoo and CNN, among others are just one notorious example. [77] These attacks effectively shut down web sites for hours and were estimated to have caused $1.2 billion in damage.[78]

To understand the sea change computer technology has introduced to criminal activity, consider a hypothetical: One can analogize a denial of service attack to using the telephone to shut down a pizza delivery business by calling the business' telephone number repeatedly, persistently and without remorse, thereby preventing any other callers from getting through to place their orders. While it may be possible for someone to execute this scheme, it would be very onerous to do so because it would require a great deal of physical effort and concentration on the perpetrator's part; he would have to be constantly dialing, maintaining the connection until it was broken and then redialing quickly to prevent any other calls from coming in. It would also involve a significant risk of apprehension because the victim could contact the authorities, who would presumably have no difficulty tracing the calls to the perpetrator, since he would presumably be using his personal or business telephone. So, while this hypothetical assault is possible, the risks involved make it exceeding unlikely to ever be carried out.

Cyberspace allows this attack to easily carry out such an attack with very little risk of apprehension. In fact, a thirteen-year old boy recently used a denial of service attack to shut down a sophisticated computer company.[79]

Like the distribution of the "Love Bug" virus, the February, 2000 denial of service attacks illustrate the tremendous reach a cybercriminal can have, in terms of number of victims targeted, amount of property destroyed or stolen,[80] and territorial area involved in the attacks. While these episodes may so

---

[76] *Criminal Threats to E-Commerce*, *supra* note 35.

[77] *See, e.g., Denial of Service Attacks*, Center for Democracy & Technology, *at* http://www.cdt.org/security/dos/ :

> A hacker can flood a computer with so many requests for data that it ceases to function and cannot provide information to legitimate requestors. This is called a `denial of service' attack because it effectively shuts down the affected computer.

[78] *See, e.g.,* Rivka Tadjer, *Detect, Deflect, Destroy*, INTERNET WEEK (Nov. 13, 2000), *at* http://www.internetweek.com/indepth/indepth111300.htm ("Roughly $100 million was in lost revenue, $100 million was the cost of additional security the victims had to add on following the attacks and a whopping $1 billion was the combined market capitalization loss").

[79] *See, e.g.,* Steve Gibson, *The Strange Tale of the Denial of Service Attacks Against GRC.COM*, http://grc.com/dos/grcdos.htm.

[80] *See Criminal Threats to E-Commerce*,*supra* note 35:

far have been the work of a single perpetrator, organized cybercrime activity targeting multiple, geographically-dispersed victims has already emerged.[81]

In addition to the increased scale it offers to criminal activity, cybercrime also has a tendency to evade traditional offense categories. While some cybercrime consists of using computer technology to commit traditional crimes such as fraud and theft, it also manifests itself as new varieties of anti-social activity that cannot be prosecuted using traditional offense categories.[82] The dissemination of the "Love Bug" virus illustrates this: the suspected author of the virus could not be prosecuted under the repertoire of offenses defined by the Philippines penal code because none of them encompassed the distribution of a computer virus, even one which destroyed property (e.g., computer files) and stole passwords.

An even better example is a denial of service attack,[83] which cannot be prosecuted as vandalism,[84] trespass,[85] burglary,[86] theft,[87] arson,[88] or extortion[89] even though it is malicious activity that damages -

---

> [E]lectrons and bits have no effective mass or weight. If one were to rob a bank or an armoured car of $2 million in cash, transportation and storage of the stolen goods would definitely be a problem. A thousand kilograms of British currency is
> hard to carry away from the bank and even more difficult to hide under a mattress. In the digital world, however, money has no weight. The theft, transportation, and storage of electron-based stolen money, or other goods for that matter, are greatly facilitated by their having no mass. $1 billion in electron from in effect weighs no more and is just as easy to transport as $10 of electrons. Thus, the potential for loss of huge amounts of cash and other goods is enormous.

[81] *See, e.g.,* Dennis Blank, *Hacker Hit Men For Hire*, BUSINESSWEEK ONLINE (May 3, 2001), http://biz.yahoo.com/bizwk/010504/dlnjckbcbkvg1r6ahnv_ua.html; D. Ian Hopper, *Large-Scale Phone Invasion Goes Unnoticed by All But FBI*, CNN.com (Dec. 14, 1999), *at* http://www.signaltonoise.net/library/phonemasters.htm.

[82] *See, e.g.,* Craig Bicknell, *Sex.Com Ruling: It Wasn't Stolen*, WIRED NEWS, (Aug. 25, 2000), *available at* http://www.wired.com/news/print/0,1294,38398,00.html:

> On Monday, U.S. District Court Judge James Ware dismissed a theft claim . . . against the convicted felon accused of hijacking sex.com, ruling that Web domains aren't property, and therefore can't be stolen.
>
> If there was a crime committed four years ago when Steven Cohen obtained sex.com by allegedly forging a bogus letter to Network Solutions authorizing the transfer of sex.com from its original owner, it wasn't theft, the judge found. Although sex.com's a solid enough piece of virtual real estate to support Cohen's now multi-million porn empire, legally, it's not real estate at all.
>
> `There is simply no evidence establishing that a domain name, including sex.com,' meets the definition of property `as required by the law of conversion,' the judge wrote in his ruling, citing his own words from a May decision in a separate suit brought by sex.com's original owner, Gary Kremen, against domain registrar Network Solutions.
>
> In the May decision, the judge sided with lawyers for Network Solutions, who argued that a domain name was not property, but rather a designation for a service -- akin to a phone number.
>
> The judge acknowledged that it's not totally clear whether property law should or shouldn't apply to Web domains, but emphasized that the job of clarifying the law rests with the legislature, not the courts. Legal experts seconded his opinion.

[83] *See, e.g.,* Eric J. Sinrod & William P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 177, 194 (2000):

perhaps even destroys - the victim's ability to conduct business.[90] No "property" is damaged; there is no intrusion into a protected area (with or without the intent to commit an offense therein); nothing is stolen (at least not in the sense that the perpetrator "takes" property from the victim and thereby enriches himself at the victim's expense); no fires or explosives are used to damage property; and nothing of value is typically extorted in exchange for ceasing the attack.[91]

Cybercrime's ability to morph into new and different forms of antisocial activity evading the reach of existing penal law creates challenges for law enforcement around the world. Cybercriminals can exploit gaps in their own country's criminal law to victimize their fellow citizens with impunity.[92] They

---

> Distributed Denial of Service attacks (DDoS) are a natural development in the search for more effective and debilitating denial of service attacks. Instead of using just one computer to launch an attack, the hacker enlists numerous computers to attack the target computer from numerous launch points. Prior to an attack, the hacker places a daemon, or a small computer program, on an innocent third-party computer. These third-party computers are often referred to as `zombies' or `soldiers.' The `slave' daemons are remotely controlled by the 'maste'" program to launch attacks against certain servers. By distributing the source of attacks across a wider array of zombie computers, the attacker has made it more difficult for the target server to block off the attack routes.

[84] *See, e.g.,* MODEL PENAL CODE § 220.3 (Proposed Official Draft 1962).

[85] *See, e.g.,* MODEL PENAL CODE § 221.2 (Proposed Official Draft 1962).

[86] *See, e.g.,* MODEL PENAL CODE § 221.1 (Proposed Official Draft 1962).

[87] *See, e.g.,* MODEL PENAL CODE § 223.2 (Proposed Official Draft 1962).

[88] *See, e.g.,* MODEL PENAL CODE § 220.1 (Proposed Official Draft 1962).

[89] *See, e.g.,* MODEL PENAL CODE § 223.4 (Proposed Official Draft 1962).

[90] *See generally* Mary M. Calkins, *They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models*, 89 GEO. L.J., 171, 180 n. 46 (2000); Sinrod & Reilly, *supra* note 83, at 199-200. The Canadian citizen accused of the high-profile denial of service attacks that occurred in February of 2000 ultimately pled guilty to five counts of "mischief to data," fifty-one counts of illegal access to a computer and one count of breach of bail conditions. *See, e.g.,* James Evans, *"Mafiaboy" Will be Sentenced in April*, NETWORK WORLD FUSION NEWS, (Jan. 22, 2001), *available at* http://www.nwfusion.com/news/2001/0122sentence.html.

As to the effects of such an attack, *see, e.g.,* Gibson, *supra* note 79 (internet security corporation's web site shut down by denial of service attack mounted by thirteen-year-old boy). *See* also Frances Ann Burns, *Hack Attack Shuts Down Online Auction Site*, apbnews.com (Sept. 12, 2000), http://www.apb.com/newscenter/breakingnews/2000/09/12/bidbay0912_01.html.

[91] It is possible to analogize a denial of service attack to vandalism. *See, e.g.,* Susan W. Brenner, *Is There Such a Thing as Virtual Crime?*, 4 CAL. CRIM. L. REV. 1 (2001), http://boalt.org/CCLR/v4/v4brenner.htm. It seems more reasonable, however, to create a new offense category targeting denial of service attacks and similar activity.

[92]In the United States, this is not uncommon with regard to cyberstalking. *See, e.g.,* U.S. Department of Justice, 1999 Report on Cyberstalking: A New Challenge for Law Enforcement and Industry, http://www.usdoj.gov:80/criminal/cybercrime/cyberstalking.htm.

For example, in *United States v. Alkhabaz*, 104 F.3d 1492 (6th Cir. 1997) a federal court of appeals upheld the trial court's dismissal of charges that Jake Baker, also known as Alkhabaz, violated 18 U.S.C. § 875 because it found he did not transmit a "credible threat" to his alleged victim. *See* 104 F.3d at 1495-1496. Baker, a student at the

can also exploit gaps in the criminal laws of other countries to victimize the citizens of those and other nations; as the "Love Bug" episode demonstrated, cybercrime is global crime.[93] The damage wreaked by

---

University of Michigan, had used e-mail to correspond with a friend; much of Baker's part of the correspondence consisted of vivid descriptions of fantasized sexual violence against a woman whose name was the same as that of one of his classmates. *See id.* at 1498 (Krupansky, J., dissenting):

> By November 1994, Baker's sadistic stories attracted the attention of an individual who called himself `Arthur Gonda,-- a Usenet service subscriber residing in Ontario, Canada, who apparently shared similarly misdirected proclivities. Baker and Gonda subsequently exchanged at least 41 private computerized electronic mail ('e-mail') communications between November 29, 1994 and January 25, 1995. Concurrently, Baker continued to distribute violent sordid tales on the electronic bulletin board. On January 9, 1995, Baker brazenly disseminated publicly, via the electronic bulletin board, a depraved torture-and-snuff story in which the victim shared the name of a female classmate of Baker's referred to below as 'Jane Doe.' . . . This imprudent act triggered notification of the University of Michigan authorities by an alarmed citizen on January 18, 1995. On the following day, Baker admitted to a University of Michigan investigator that he had authored the story and published it on the Internet.

When the correspondence came to light, Baker was prosecuted under for sending "threats" via interstate commerce. *See id.* at 1493. The district court dismissed the charge because it found that the e-mail correspondence did not constitute "true threats" and was therefore speech protected by the First Amendment to the U.S. Constitution. *See id.* The Sixth Circuit affirmed the dismissal because it agreed that the e-mail correspondence did not rise to the level of a "threat":

> [W]e hold that, to constitute 'a communication containing a threat' under Section 875(c), a communication must be such that a reasonable person (1) would take the statement as a serious expression of an intention to inflict bodily harm (the mens rea), and (2) would perceive such expression as being communicated to effect some change or achieve some goal through intimidation (the actus reus). . . . [W]e conclude that the communications between Baker and Gonda do not constitute `communications containing a threat' under Section 875(c). Even if a reasonable person would take the communications between Baker and Gonda as serious expressions of an intention to inflict bodily harm, no reasonable person would perceive such communications as being conveyed to effect some change or achieve some goal through intimidation. Quite the opposite, Baker and Gonda apparently sent e-mail messages to each other in an attempt to foster a friendship based on shared sexual fantasies.

See id. at 1495-96.

[93]For another example of this, *see, e.g.,* Burns, *supra* note 90:

> A California-based online auction site has offered a $25,000 reward for information on the perpetrators of an apparent hacker attack that put the site out of business for hours.
>
> George Tannous, founder and chief executive officer of BidBay.com, said the attack occurred at a bad time, when thousands of new registered users were being welcomed. He described the attacks as sporadic and said they halted after BidBay technicians took down two servers, deleted and reinstalled software and created a firewall. . . .
>
> Last Thursday, BidBay's servers were overwhelmed by millions of messages apparently coming from an Internet service provider in Bulgaria, Tannous said. On Friday, the attacks apparently came from Austria. But the perpetrator could be anywhere in the world.

the "Love Bug" may have been to some extent inadvertent;[94] if that is true, imagine what a cybercriminal dedicated to wreaking global havoc could achieve. As a memorandum from the Council of Europe's Committee of Experts on Crime in Cyber-Space explains:

> [the] revolution in information technologies has changed society fundamentally and will probably continue to do so in the foreseeable future. . . . .
>
> . . . . Classical telephony, involving the transmission of human voice, has been overtaken by the exchange of vast amounts of data, comprising voice, text, music and static and moving pictures. This exchange no longer occurs only between human beings, but also between human beings and computers, and between computers themselves. . . .
>
> . . . The ease of accessibility and searchability of information contained in computer systems, combined with the practically unlimited possibilities for its exchange and dissemination, regardless of geographical distances, has lead to an explosive growth in the amount of information available. . . .
>
> . . . These developments have given rise to an unprecedented economic and social changes, but they also have a dark side: the emergence of new types of crime as well as the commission of traditional crimes by means of new technologies. Moreover, the consequences of criminal behaviour can be more far-reaching than before because they are not restricted by geographical limitations or national boundaries. The recent spread of detrimental computer viruses all over the world has provided proof of this reality. . . .
>
> . . . The new technologies challenge existing legal concepts. Information and communications flow more easily around the world. Borders are no longer boundaries to this flow. Criminals are increasingly located in places other than where their acts produce their effects. However, domestic laws are generally confined to a specific territory. . . .[95]

C. INCIDENCE AND COSTS OF CYBERCRIME

> Undeterred by the prospect of arrest or prosecution, cyber criminals around the world lurk on the Net as an omnipresent menace to the financial health of businesses, to the trust of their customers, and as an emerging threat to nations' security. According to the Computer Emergency Response Team Coordination Center . . . the number of reported incidences of security breaches in the first three quarters of 2000 rose by 54 percent over the total number of reported incidences in 1999. Moreover, countless instances of illegal access and damage around the world remain unreported, as victims fear the exposure of vulnerabilities, the potential for copycat crimes, and the loss of public confidence.[96]

---

[94] *See, e.g.,* Dirk Beveridge, *Filipino Student Says Love Bug An Accident,* THE TIMES OF INDIA, (May 12, 2000), http://www.timesofindia.com/120500/12home7.htm.

[95] COUNCIL OF EUROPE, COMMITTEE OF EXPERTS ON CRIME IN CYBER-SPACE, EXPLANATORY MEMORANDUM TO THE DRAFT CONVENTION ON CYBER-CRIME, ¶¶ 1-6 (May 25, 2001), http://conventions.coe.int/Treaty/EN/cadreprojets.htm [hereinafter EXPLANATORY MEMORANDUM].

[96] *Combating Cybercrime: A Proactive Approach*, MCCONNELL INTERNATIONAL, E-LERT NUMBER 2 (Feb. 2001), http://www.mcconnellinternational.com/pressroom/elert2.cfm (footnote omitted).

There are, unfortunately, no surveys documenting the incidence of cybercrime at the global level.[97] The results of national surveys, however, bear out the picture given in the quotation above: cybercrime is consistently and dramatically increasing.[98]

The most-often cited national survey for the United States is the "Computer Crime and Security Survey," which was conducted by the Computer Security Institute with participation by the FBI's Computer Intrusion Squad, San Francisco branch.[99] The CSI/FBI survey, conducted annually since 1996, reports results of data obtained from several thousand information security professionals employed by corporations, financial institutions, government agencies and universities.[100] One area the survey explores is security breaches: whether respondents have experienced breaches of information security in the last year.[101] The number responding in the affirmative has grown over the years: in the 2001 survey, 85% of respondents said they had detected breaches over the last year; only 42% of 1996 survey respondents reported detection of such breaches.[102]Among other things, the survey shows (a) that the Internet continues to become an increased point of attack,[103] (b) that denial

---

[97] *See, e.g., id*. at n. 1.

[98] Other surveys focus not on the incidence of cybercrime, but on the extent to which the public is concerned about cybercrime, perhaps on the theory that public opinion is an important driver of national policy. The results of such a survey released in April of 2001 showed that

> Americans are deeply worried about criminal activity on the Internet, and their revulsion at child pornography is by far their biggest fear. Some 92% of Americans say they are concerned about child pornography on the Internet and 50% of Americans cite child porn as the single most heinous crime that takes place online.
>
> In other areas, 87% of Americans say they are concerned about credit card theft online; 82% are concerned about how organized terrorists can wreak havoc with Internet tools; 80% fear that the Internet can be used to commit wide scale fraud; 78% fear hackers getting access to government computer networks; 76% fear hackers getting access to business networks; and 70% are anxious about criminals or pranksters sending out computer viruses that alter or wipe out personal computer files.

The responses came from 2,096 Americans who were surveyed in February and March of 2001; 1,198 of the respondents are Internet users. PEW INTERNET & AMERICAN LIFE, FEAR OF ONLINE CRIME (April 5, 2001), http://www.pewinternet.org/reports/reports.asp?Report=32&Section=ReportLevel1&Field=Level1ID&ID=117.

[99] *See Financial Losses Due to Internet Intrusions, Trade Secret Theft and Other Cyber Crimes Soar*, COMPUTER SECURITY INSTITUTE (Mar. 12, 2001), http://www.gocsi.com/prelea_000321.htm.

[100]CSI/FBI 2000 COMPUTER CRIME AND SECURITY SURVEY, http://cbc.ca/news/indepth/hackers/csi-fbi2000.pdf. Questionnaires were sent to 4,284 information security professionals in 2000 and 1999, with a response rate of 15% (643 responses) in 2000, 14% (521 responses) in 1999. *Id.* The response rate for 1998 was 13% (520 responses out of 3,890 questionnaires distributed), 11.49% in 1997 (563 responses out of 4,899 questionnaires) and 8.6% in 1996 (428 responses out of 4,971 questionnaires distributed). *Id.*

[101] *See Financial Losses Due to Internet Intrusions, Trade Secret Theft and Other Cyber Crimes Soar*, *supra* note 99.

[102]*See* CSI/FBI 2001 COMPUTER CRIME AND SECURITY SURVEY, http://cbc.ca/news/indepth/hackers/csi-fbi2000.pdf; CSI/FBI 2000 COMPUTER CRIME AND SECURITY SURVEY, *supra* note 100.

[103] In the 2001 survey, 70% reported that the Internet was a frequent point of attack, while only 59% reported this in the 2000 survey. *See id. See also Financial Losses Due to Internet Intrusions, Trade Secret Theft and Other Cyber*

of service attacks are increasing and[104] (c) that viruses are becoming increasingly common.[105] Those responding to the CSI/FBI survey are also asked to quantify the losses they attribute to cybercrime. The figure reported rose from $100,119,555 in the 1997 survey to $377,828,700 in the 2001 survey.[106]

Data from other countries reveal similar trends.[107] "Cybercrime accounted for half of all fraud committed in the UK in the first six months" of 2000, and there was "a 56 per cent increase in hacking in the UK over the past 12 months, with most hackers seeking financial gain, for example by using their hack to demand money, or for political reasons such as posting messages for a certain cause on a company's website."[108] Statistics from China and Japan also showed dramatic increases in cybercrime,[109]

Crimes Soar, *supra* note 99 ("For the fourth year in a row, more respondents . . . cited their Internet connection as a frequent point of attack than cited their internal systems. . . .").

[104] Thirty-eight per cent of those responding to the 2001 survey had detected denial of service attacks, while only 27% of those responding to the 2000 survey reported detecting such attacks. *See id.*

[105]Ninety-four per cent of those responding to the 2001 survey had detected computer viruses. *See id.*

[106]*See id.* Of course, some maintain that it is difficult to calculate the amount of loss attributable to cybercrime. *See, e.g.,* Ronald B. Standler, *Computer Crime* (1999), http://www.rbs2.com/ccrime.htm.

[107] Many countries have not compiled cybercrime statistics and at least one, the United Kingdom, has chosen not to do so. *See, e.g.,* Wendy McAuliffe, *Home Office Says "No" To Cybercrime Figures*, ZDNET UK, (Apr. 20, 2001), http://news.zdnet.co.uk/story/0,,s2085752,00.html:

> The Home Office will not be recording cybercrime figures, despite investing £25m in a National High-Tech Crime Unit (NHTCU) launched on Wednesday. . . .
>
> Despite the Home Office's commitment to tackling computer-based crime, it has no plans to gather or publish official cybercrime figures in the future.
>
> `We do not intend to distinguish the way in which crimes are committed -- an offence is the same whether it is committed on or offline,' said a Home Office spokesperson. . . .
>
> This seems to contradict the police's desire to find out how much criminal activity is going on online. Launching the NHTCU, deputy director general of NCIS Roger Gaspar admitted his concern over the lack of statistical evidence available on cybercrime.
>
> `One of the issues law enforcement faces is that the true extent of IT-based criminality is as yet uncertain because no statistics have been collated hitherto. . . .' he said at the launch. . . .
>
> According to the Home Office, number-crunching is not necessary to prove the growth of Internet offences. . . .

[108] Jo Ticehurst, *Cybercrime Soars in the UK*, VNUNET.COM, (June 11, 2000), http://www.vnunet.com/News/1113497.

[109] *See* M.E. Kabay, *Studies and Surveys of Computer Crime*, SECURITY PORTAL, (Dec. 12, 2000), http://www.securityportal.com/cover/coverstory20001211.html:

> The official Xinhua news agency reported that computer crime has been exploding in the People's Republic of China. The annual growth rate of 30% led to over 100 recorded cases of computer-related crimes in 1998 with estimates of undetected crime running about 6:1, with a projected rates of 600 crimes in 1998 in the PRC. One Chinese estimate guessed that 95% of all PRC Websites

and the Australian version of the CSI/FBI survey found that "one third . . . of the companies surveyed reported an attack in the last 12 months."[110] When those responding to this survey were asked about the future, the number "who indicated that increased virtual crime is a concern almost doubled," and those reporting "concern about the shift from conventional crimes against property to computer related crimes more than doubled."

The value of these surveys is perhaps more anecdotal than scientific. As almost everyone concedes, it is difficult to gather accurate cybercrime statistics. One problem in gathering data about the commission of cybercrimes is that:

> an unknown number of crimes of all kinds are undetected. For example, even outside the computer crime field, we don't know how many financial frauds are being perpetrated. We don't know because some of them are not detected. How do we know they're not detected? Because some frauds are discovered long after they have occurred. Similarly, computer crimes may not be detected by their victims. . . .
>
> A commonly-held view within the information security community is that only one-tenth or so of all the crimes committed against and using computer systems are detected.[111]

These detection problems suggest that such surveys seriously underestimate the incidence of cybercrime, a premise supported by another factor as well, the underreporting of cybercrime:

> [E]ven if attacks are detected, it seems that few are reported in a way that allows systematic data collection. This belief is based in part on the unquantified experience of information security professionals who have conducted interviews of their clients; it turns out that only about ten percent of the attacks against computer systems revealed in such interviews were ever reported to

---

> have been penetrated by local and overseas criminal hackers because of the relatively weak level of security in the PRC. . . .
>
> In Japan, the National Police Agency reported in February that computer crime was up 58% in 1998 compared with 1997 — a 1300% growth since the first statistics were kept in 1993. Specific crimes increased even more than the aggregate average; e.g., forgery and data diddling cases grew 67% in 1998. . . .
>
> The Chinese Department of Public Security announced that it had solved 100 cases of criminal hacking in 1998 but estimated that this was only about 15% of the actual level of unauthorized system access. Reported computer crime was growing at an annual rate of 30%, they said. About 95% of all Chinese systems on the Internet had been attacked last year, with many banks and other financial institutions the target of Chinese and international criminals. . . .

[110] DELOITTE AND VICTORIA POLICE COMPUTER CRIME SURVEY 1999, *available at* http://www.deloitte.com.au/internet/item.asp?id=3140. The Australian survey found that the

> attacks perpetuated appear to be random, "spur of the moment" attacks, with no discernible pattern detected in more than 75% of the cases. According to respondents, the most likely motivation for an attack was curiosity (71%). The attacker was most likely to be a disgruntled employee or an independent hacker.

Id.

[111] *See* Kabay, *supra* note 109. *Accord Conclusions of the Study on Effective Measures to Prevent and Control High-Technology and Computer-Related Crime, supra* note 30, item 34 at 10.

> any kind of authority. . . . Department of Defense studies . . . were consistent with this belief; of the few penetrations detected, only a fraction of one percent were reported to appropriate authorities.[112]

Some of the reasons for the under-reporting of cybercrime are that "victims . . . may not realize that the conduct involved is a crime, or may decide not to complain for reasons of embarrassment or corporate credibility."[113]

> There are other impediments to the compilation of accurate cybercrime statistics:
>
> Further problems arise with the mass victimization caused by offences such as virus propagation, because the numbers of victims are simply too large to identify and count, and because such programs can continue creating new victims long after the offenders have been caught and punished. A further factor complicating the gathering and comparison of national crime statistics will be the fact that transnational computer-related crimes are, by definition, committed in or have effects in at least two States, and, in some cases, in many States, risking multiple reporting or no reporting at all.[114]

Methodological problems with the compilation of cybercrime statistics lie in certain of the techniques used to gather information, but do not cut clearly in favor of either under- or overestimating the incidence of cybercrime. So far, much of the information we have on cybercrime is the product of surveys directed toward individuals working in the field of information security.[115] The information elicited by these surveys may be skewed by biases in the selection of the respondents and/or distortions in the language used in the survey instruments.[116]

---

[112] Kabay, *supra* note 109. *See* DELOITTE AND VICTORIA POLICE COMPUTER CRIME SURVEY 1999, , *supra* note 114. The CSI/FBI surveys, on the other hand, have found an increasing tendency to report cybercrimes to law enforcement authorities. *See Financial Losses Due to Internet Intrusions, Trade Secret Theft and Other Cyber Crimes Soar*, *supra* note 99:

> Thirty-six percent of respondents reported the intrusions to law enforcement; a significant increase from 2000, when only 25% reported them. (In 1996, only 16% acknowledged reporting intrusions to law enforcement.)

[113] *Conclusions of the Study on Effective Measures to Prevent and Control High-Technology and Computer-Related Crime, supra* note 30, item 34 at 10.

[114] *Id.,* item 34 at 10-11.

[115] CSI/FBI 2001 COMPUTER CRIME AND SECURITY SURVEY, *supra* note 102; DELOITTE AND VICTORIA POLICE COMPUTER CRIME SURVEY 1999, *supra* note 110.

[116] Kabay, *supra* note 109:

> The critical issue when considering the reliability of surveys is *self-selection* bias — the obvious problem that survey results include only the responses of people who agreed to participate. Before basing critical decisions on survey data, it is useful to find out what the response rate was; although there are no absolutes, in general we tend to trust survey results more when the response rate is high. Unfortunately, response rates for telephone surveys are often less than 10%. . . . It is very difficult to make any case for random sampling under such circumstances, and all results from such low-response-rate surveys should be viewed as indicating the range of problems or experiences of the respondents rather than as indicators of population statistics.

As noted above, the response rate for the CSI/FBI survey roughly ranges between 11-15%. *See* CSI/FBI 2000 COMPUTER CRIME AND SECURITY SURVEY, *supra* note 100.

Other, presumably more reliable information about the incidence of cybercrime comes from organizations that track computer intrusions. The Computer Emergency Response Team Coordination Center (CERT/CC), for example, is a government funded computer security research center at Carnegie Mellon University.[117] CERT/CC tracks and issues reports on computer "incidents," which it defines as "`any related set of activities.'"[118] Under this definition, a large-scale episode such as the "Love Bug" virus outbreak counts as one incident, just as a smaller event also counts as one.[119] At the end of April, 2001, CERT/CC reported that for the first quarter of 2001 it received "7,047 incident reports, putting 2001 on pace to eclipse 2000's total of 21,756." Incident reports filed with CERT/CC have increased annually over the last several years, indicating a corresponding increase in cybercrime activity.[120]

Another source of information on the incidence of cybercrime is law enforcement, which is charged with investigating offenses and apprehending the perpetrators. In his March 28, 2000 testimony before the U.S. Senate Committee on the Judiciary's Subcommittee for Technology, Terrorism and Government Information, FBI Director Louis J. Freeh explained:

> [as] Internet use continues to soar, cyber crime is also increasing exponentially. As I mentioned earlier, our case load reflects this growth. In FY 1998, we opened 547 computer intrusion cases; in FY 1999, that number jumped to 1154. Similarly, the number of pending cases increased from 206 at the end of FY 1997, to 601 at the end of FY 1998, to 834 at the end of FY 99, and to over 900 currently. These statistics include only computer intrusion cases, and do not account for computer facilitated crimes such as Internet fraud, child pornography, or e-mail extortion efforts. In these cases, the NIPC and NIPCI squads often provide technical assistance to traditional investigative programs responsible for these categories of crime.[121]

Mr. Freeh also said he expected "these upward trends" in the commission of cybercrime to continue.[122]

There is yet another reason for the uncertainty regarding cybercrime incidence: because of a lack of consensus as to definitions of cybercrime police cannot keep accurate track of it.[123] This means law enforcement agencies cannot aggregate data on the commission of cybercrime.[124] Law enforcement agencies thus can neither justify expending resources to combat the problem nor conduct trend and other analyses essential to devising a planned response to the problem cybercrime poses.[125]

---

[117] *See The CERT® Coordination Center FAQ*, *at* http://www.cert.org/faq/cert_faq.html.

[118] Sam Costello, *CERT Statistics Point to Increasing Security Woes*, CNN.COM, (Apr. 30, 2001), *at* http://www.cnn.com/2001/TECH/internet/04/30/cert.security.stats.idg/index.html.

[119] *See id.*

[120] *See id.*

[121] Freeh, *supra* note 47.

[122] *See id.*

[123] *See, e.g.,* Marc D. Goodman, *Making Computer Crime Count,* FBI LAW ENFORCEMENT BULLETIN (July 2001).

[124] *See id.*

[125] *See id.*

As to the problems posed by cybercrime, the Gartner Group estimates that "the financial damage caused by cybercrime will increase by between 1000 and 10,000 per cent by 2004."[126] Another report found cybercrime "already a multi-billion dollar business."[127] However, as a United Nations report explains, the financial costs of cybercrime are not only hard to estimate, but financial costs themselves represent less than all the damage this type of activity inflicts:

> Actual losses are difficult to quantify, but include direct costs of repairing systems and software, the loss of access or services to users and consequent damage, the loss of valuable data and the loss of revenue from site operations. Such crimes also necessitate the development and maintenance of security and other preventive measures, an added cost factor. The overall increases in such crime and the spectacular nature of some of the offences involved also generate substantial but unpredictable political pressures for the enhancement of criminal law controls, more severe punishments and technical precautions on the part of the producers of software and hardware and of companies that provide network access to customers. A further hidden cost of such incidents is the fear of cybercrime, which may erode usage of the technologies or deter Governments and populations in developing countries from making the most effective use of them.[128]

As to the incidence and effects of cybercrime, it is safe to agree with the position taken by the European Commission in launching its cybercrime initiative: while conceding "there are no reliable statistics on cybercrime," the Commission pointed out "`there is little doubt that these offences constitute a threat to industry investment and assets, and to safety and confidence in the information society.'"[129]

The United Nations expressed similar views:

> There are few comprehensive statistics concerning high-technology or computer-related crime, but anecdotal evidence and such statistics as are available suggest that the extent of such crime is increasing with the growing number of potential offenders and victims online. The range of criminal activities also appears to be expanding as technologies create new criminal opportunities and offenders find new ways to exploit them. Of particular concern currently is the rapid expansion of electronic commerce and its supporting infrastructure, which are likely to be accompanied by subsequent increases in economic computer-related crimes such as fraud, the manipulation of financial markets and money-laundering.[130]

---

[126] Aled Miles, *Bug Watch: The Fight Against Cybercrime*, VNUNET.COM, (Apr. 20, 2001), *at* http://theconnection.vnunet.com/News/1120814 (Gartner Group prediction). *See also* Barb Gomolski, *Cybercrime More Than Just a Pesky Computer Virus*, ITWORLD.COM, (Mar. 23, 2001), *at* http://www.itworld.com/Sec/3495/IWD010326opgartner/ (Gartner Group also predicts that "cybercrime will increase by two or three orders of magnitude by 2004").

[127] Borchgrave, *supra* note 55,at iv ("At a Berlin conference of 100 Internet experts from the G8 group of industrialized nations in late October, German Foreign Minister Joschka Fischer said cybercrime losses have reached 100 billion German marks ($42.9 billion) for the eight major countries, including the U.S.").

[128] *Conclusions of the Study on Effective Measures to Prevent and Control High-Technology and Computer-Related Crime, supra* note 30, item 32 at 10.

[129] Jelle van Buuren, *European Commission Wants to Tackle Cybercrime*, TELEPOLIS, (Jan. 10, 2001), http://www.heise.de/tp/english/special/enfo/4658/1.html.

[130] *Conclusions of the Study on Effective Measures to Prevent and Control High-Technology and Computer-Related Crime, supra* note 30, item 30 at 10 (footnote omitted).

III. WHAT MEASURES ARE BEING TAKEN TO COMBAT CYBERCRIME AT THE NATIONAL AND INTERNATIONAL LEVELS?

> *Since the 1970s, there has been a growing consensus that existing criminal laws covering the variety of crimes that can be committed with a computer . . . either do not cover some computer abuses or are not strong and clear enough to discourage computer crimes and allow expeditious prosecution.*[131]

The preceding section accomplished the definition of cybercrime. We now turn to what must be done in terms of developing criminal laws strong, clear and consistent enough[132] to discourage engagement in cybercrime and to allow for expeditious investigation and prosecution of the undeterred. Section III(A) reviews what has been done in this regard at the national and international levels; Section III(B) examines efforts to develop a repertoire of consensus crimes and use them as the platform for establishing international strategies against cybercrime; Section III(C) examines additional measures that can be taken to achieve this end; Section III(D) assesses the likelihood of success in developing an effective global strategy against cybercrime.

A. A BRIEF CHRONOLOGY: NATIONAL AND INTERNATIONAL EFFORTS

> *[C]omputer-related crime requires the identification of entirely new offences and the modification of existing offences to ensure that they extend to misuses of the new technologies. . . . . International consensus is emerging with respect to a substantial core of the most serious and harmful conduct, but some areas remain which are treated as crimes by some States but not all.*[133]

1. *THE ORIGINS OF COMPUTER CRIME AND NATIONAL LEGISLATION: 1960'S-1970'S*

The history of computer-related crime begins with the history of computers. The first published accounts of computer manipulation, sabotage, espionage, and the illegal use of computer systems date back to the published press and scientific literature of the 1960s.[134] These early computer crimes differed in type and scale from cybercrimes:

---

[131] U.S. CONGRESS, OFFICE OF TECHNOLOGY ASSESSMENT, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: MANAGEMENT, SECURITY, AND CONGRESSIONAL OVERSIGHT 85 (1986), http://www.ota.nap.edu/pdf/data/1986/8611.PDF.

[132] *See* § III(B), *infra*.

[133] *Conclusions of the Study on Effective Measures to Prevent and Control High-Technology and Computer-Related Crime, supra* note 30, item 14.

[134] *See, e.g.,* ULRICK SIEBER, LEGAL ASPECTS OF COMPUTER-RELATED CRIME IN THE INFORMATION SOCIETY, COMCRIME Study prepared for the European Commission 19 (Jan. 1998), http://europa.eu.int/ISPO/legal/en/comcrime/sieber.doc:

> Early computers were dedicated mainframes -- and users were generally directly wired into the computers. Thus, early computer crime cases were characterized by authorized users manipulating computer programs to, for example, steal money from a bank or other employer.
>
> Other typical early computer crimes included attacks on telephone systems and networks . . . or diversion of money through electronic funds transfers. Because early users of computers were highly centralized and not very interconnected, the opportunity for computer crime tended to be limited to misuse of systems by authorized users. The nature of early computer offenses likewise was limited by the talents of the users and the nature of the non-distributed computer systems.
>
> . . . [P]rosecutors and judges were forced to deal with computer miscreants by resorting to ordinary criminal law concepts of theft, destruction of property, trespass and criminal mischief. At that time, computers tended to be large, dedicated stand-alone machines, and access . . . was generally restricted by limiting access to the physical terminals which were connected to the mainframe computer. As a result, virtually all computer crimes were committed by insiders or quasi-insiders. Legitimate computer users with authorized access to the computers, software developers, vendors and other authorized users were the primary perpetrators of these computer crimes. . . . .[135]

The first empirical computer crime studies to apply criminological research methods were conducted in the 1970s. These studies verified a limited number of cases, suggesting that many more have gone undetected or unreported.[136]

In the United States, the Senate Governmental Affairs Committee held hearings on the need for computer crime legislation in 1976,[137] which prompted Senator Abraham Ribicoff in 1977 to introduce the Federal Computer Systems Protection Act as the first proposal for federal computer crime legislation.[138] The bill, revised and reintroduced in 1979,[139] declared any "knowing, willful manipulation or attempted manipulation: of "any computer owned or operated by the United States, certain financial institutions, and entities affecting interstate commerce, for the purpose of `devising or executing any

---

> The history of `computer crime' dates back to the 1960s when first articles on cases of so-called "computer crime" or `computer-related crime' were published in the public press and in scientific literature. These cases primarily included computer manipulation, computer sabotage, computer espionage and the illegal use of computer systems. However, due to the fact that most reports were based on newspaper clippings, it was controversially discussed whether or not this new phenomenon of computer crime had any plausible reasons.

(footnotes omitted).

[135] MARK D. RASCH, THE INTERNET AND BUSINESS: A LAWYER'S GUIDE TO THE EMERGING LEGAL ISSUES, Chapter 11 (*Criminal Law and the Internet*) § II (1995), *available at* http://www.swiss.ai.mit.edu/6805/articles/computer-crime/rasch-criminal-law.html.

[136] SIEBER, *supra* note 134.

[137] *See* Robin K. Kutz, Note, *Computer Crime In Virginia: A Critical Examination Of The Criminal Offenses In The Virginia Computer Crimes Act,,* 27 WM. & MARY L. REV 783, 787 (1986).

[138] *See* Federal Computer Systems Protection Act, S. 1766, 95th Cong., 1st Sess., 123 CONG. REC. 21,025 (1977). *See also* Joseph M. Olivenbaum, *Ctrl-Alt-Delete: Rethinking Federal Computer Crime Legislation*, 27 SETON HALL L. REV. 574, 584, n. 32 (1997) (quoting S. 240, 96th Cong. (1979)).

[139] Olivenbaum, *supra* note 138.

scheme or artifice to defraud,' or of `obtaining money, property, or services...by means of false or fraudulent pretenses, representations, or promises'" to be "a crime and could have a jail sentence of up to 15 years."[140] The 1979 bill died in committee,[141] but it was influential in promoting the subsequent enactment of federal computer crime legislation and in encouraging the adoption of such legislation in two states, Arizona and Florida.[142]

The 1980s witnessed cases of hacking, viruses, and worms, as well as program piracy, cash dispenser manipulation and telecommunication abuses. Vulnerabilities of an information-based society and limitations of existing computer security approaches, as well as the limitations of law and enforcement efforts were widely publicized in the 1990s. Computer crime has expanded in scope far beyond mere economic crime, and can be expected to include attacks against national infrastructure, security and social well being.[143]

Computer-related criminal law has undergone similar changes, in response to the criminal evolution enabled and enhanced by information technology. Legal reforms have taken place in many countries (mostly European) since the 1970s, reflecting not only changes in technology, but also a change in legal paradigms. Prior to the mid-twentieth century, all countries' criminal codes focused principally on the protection of tangible objects. However, the emergence of an information-based society placing great value and dependence on incorporeal values and information has predicated the development of new laws to protect incorporeal values.[144]

2. THE MAIN WAVES OF NATIONAL LEGISLATION: 1970'S-1990'S

The first wave of law reform in most western legal systems addressed the protection of privacy, in response to emerging vast capabilities for collecting, storing and transmitting data by computer equipment.[145] Administrative, penal and civil legislation was enacted to protect data and associated citizens' rights to privacy the following countries: Sweden (1973); the United States of America (1974); the Federal Republic of German (1977); Austria, Denmark, France and Norway (1978); Luxembourg (1979 and 1982); Iceland and Israel (1981); Australia and Canada (1982); the United Kingdom (1984); Finland (1987); Ireland, Japan and the Netherlands (1988); Portugal (1991); Belgium, Spain and

---

[140] Glenn D. Baker, Note, *Trespassers Will Be Prosecuted: Computer Crime in the 1990s*, 12 COMPUTER L.J. 61, 63 n.15 (1993); Olivenbaum, *supra* note 138.

[141] Dodd S. Griffith, Note, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAND. L. REV. 453,485 n. 277 (1990). Apparently, one of the concerns was that the measure "expanded Federal jurisdiction too broadly." U.S. CONGRESS, OFFICE OF TECHNOLOGY ASSESSMENT, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: MANAGEMENT, SECURITY, AND CONGRESSIONAL OVERSIGHT 88 (1986), *available at* http://www.ota.nap.edu/pdf/data/1986/8611.PDF

[142] *See, e.g.,* Kutz , *supra* note 137, at 789 (Arizona enacted computer crime legislation in 1978); Lynn Becker, *Electronic Publishing: First Amendment Issues in the Twenty-First Century*, 13 FORDHAM URB. L.J. 801, 703 n.7 (1984/1985) (Florida adopted computer crime legislation in 1979).

[143] SIEBER, *supra* note 134, at sec. I.A.1, Historical Development and Definition.

[144] *Id.* at sec. I.B., The Concept of Computer-Related Criminal Law.

[145] *Id.* at sec. I.A.1.

Switzerland (1992); Spain (1995); Italy and Greece (1997).[146] This concern with privacy prompted constitutional amendments in Brazil, the Netherlands, Portugal and Spain.[147]

The second wave of computer-related law reform originated in the 1980s and encompassed economic crimes.[148] This wave was precipitated by the inadequacy of the existing traditional criminal provisions, which protect exclusively physical, tangible and visible objects against traditional crimes, in the advent of cybercrime.[149] The new laws addressed the new capabilities of computer related crimes to violate traditional objects through new media (such as stealing money by manipulating bank accounts), to involve intangible objects (such as computer programs), and to employ new methods of committing crimes made possible by increasing use and reliance on computer systems and networks.[150] The following countries enacted new laws against computer-related economic crimes (including provisions against illegal access to computer systems) to deal with the new criminal realities: Italy (1978); Australia (state law, 1979); United Kingdom (1981, 1990); United States of America (federal and state legislation in the 1980's);[151] Canada and Denmark (1985); the Federal Republic of Germany and Sweden (1986);

---

[146] *Id.*

> The first wave of law reform in most western legal systems emerged in the field of privacy protection in the 1970s and 1980s. This legislation was a reaction to new challenges of privacy caused by expanded possibilities for collecting, storing and transmitting data by new technologies. `Data protection laws' were enacted . . . protecting the citizens' right of privacy with administrative, civil, and penal regulations in 1973 in Sweden, 1974 in the United States of America, 1977 in the Federal Republic of Germany, 1978 in Austria, Denmark, France and Norway, 1979 and 1982 in Luxembourg, 1981 in Iceland and Israel, 1982 in Australia and Canada, 1984 in the United Kingdom, 1987 in Finland, 1988 in Ireland, Japan and the Netherlands, 1991 in Portugal, 1992 in Belgium, Spain and Switzerland, 1995 in Spain, and 1997 in Italy and Greece.

(footnote omitted).

[147] SIEBER, *supra* note 134 (citing Article 5(O)X, Brazil Constitution; Article 10, Constitution of the Netherlands; Article 35 of the Constitution of Portugal; and Article 18.4 of the Constitution of Spain).

[148] *Id.*

[149] *Id.*.

[150] *Id.*

[151] *See, e.g.,* Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. 98-473, Title II, § 2102(a), (Oct. 12, 1984) (codified as 18 U.S. Code § 1030).

> The 1984 Act . . . . prohibited the accessing of computers in three areas. The first section . . . made it a felony to knowingly access a computer without authorization for the purpose of gaining information relating to United States defense or foreign relations with the intent of causing injury to the United States or giving an advantage to a foreign nation. The second section made it a misdemeanor to knowingly access a computer without authorization to obtain financial information contained in the record of a financial institution or a consumer reporting agency. The statute also made it a misdemeanor to knowingly access a computer without authorization in order to use, modify, destroy or disclose information in or prevent the authorized use of the computer with the knowledge that the computer is operated for or on behalf of the United States and would affect the government's operation of the computer.
>
> The 1984 Act contained penalties of up to ten thousand dollars or imprisonment of up to ten years

Austria, Japan and Norway (1987); France and Greece (1988); Finland (1990, 1995); the Netherlands (1992); Luxembourg (1993); Switzerland (1994); Spain (1995); and Malaysia (1997).[152]

A third wave of amendments and additions to national laws also took place in the 1980s.[153] This effort was directed toward providing better protection of intellectual property in the realm of computer

---

> for the most serious first time offender of the classified information subsection and penalties were increased for repeat offenders of this subsection, with a maximum of twenty years imprisonment and a one hundred thousand dollar fine. The misdemeanor offenses carried a penalty of five thousand dollars or imprisonment for not more than one year.

Baker, *supra* note 140, at 64-65 (footnotes omitted). The 1984 Act was amended in 1994 to:

> deal with the problem of computer viruses. By focusing almost exclusively on the authorization of the user to access a computer, the CFAA failed to adequately examine the problem of what types of criminal conduct people could do to computer without "accessing" such a computer. Because the structure of the computer crime statute focused upon the unauthorized access, and not upon the later use of the computer, legislative reform was necessary to deal with the problem.
>
> The amended computer crime law punishes those who, without the knowledge and authorization of the "persons or entities who own or are responsible for" a computer, cause the transmission of "a program, information, code, or command to a computer or computer system" with the intent to cause damage to the computer or information in the computer or prevent the use of the system.
>
> In addition to punishing intentional conduct, the statute criminalizes those who act "with reckless disregard of a substantial and unjustifiable risk" of damage or loss, and would create a civil cause of action for `any person who suffers damage or loss by reason of a violation of the section' to obtain compensatory damages or injunctive relief.

RASCH, *supra* note 135 (footnotes omitted, quoting 18 U.S. Code § 1030(a)(5)(A)-(B). For the text of the amending enactment *see* Public L. 103-322, Title XXIX, § 290001(b)-(f), 108 Stat. 2097. Sept. 13, 1994.

> By 1986, forty-five states had enacted some cybercrime legislation. *See* Kutz, *supra* note 137, at 789.
>
> Twenty-three of these states apparently modeled their statutes primarily on the 1977 or 1979 versions of the proposed Federal Computer Systems Protection Act, while twenty enacted comprehensive computer-assisted crime statutes less closely related to the proposed federal legislation. The other two states, Ohio and Massachusetts, took another tack, choosing only to redefine certain terms in their criminal codes to ensure that their statutes covered computers and computer-related intangible property. Ohio took the more expansive approach, by expanding its definitions of `property,' `services,' and `writing,' and by adding six new computer-related definitions, while Massachusetts chose only to redefine the term `property' in its larceny statute to include computer-related intangibles.

Id. at 789-790 (footnotes omitted). By 2000, every state had adopted some form of cybercrime legislation, much of which tended to focus on the computer intrusion offenses, e.g., hacking and cracking. *See, e.g.,* Shell Draft, Model State Computer Crimes Code, *at* http://www.cybercrimes.net/ShellDraft/MSCCCShellDraft.html.

[152] *See* SIEBER, *supra* note 134.

[153] *Id.*

technology.[154] These laws include copyright protection for computer programs, including criminal copyright law and legal protection of topographies.[155]

National legislation concerning illegal and harmful content emerged as a fourth wave in the 1980s.[156] This type of legislation began to expand significantly with the ubiquity of the Internet, beginning in the mid-1990s.[157] Content-related legislation has covered such topics as dissemination of pornography and pedophilia, hate speech and defamation, and the responsibility of service and access providers.[158] The nature of content deemed illegal as well as methods for enforcement vary significantly according to national attitudes and legal systems.

3. CHRONOLOGY OF INTERNATIONAL EFFORTS

Various international and supranational organizations have recognized the inherently transborder nature of cybercrime, the ensuing limitations of unilateral approaches, and the need for international harmonization of legal, technical, and other solutions. In particular, the Organisation for Economic Co-operation and Development (OECD),[159] the Council of Europe,[160] the European Union,[161] the United

---

[154] *Id.*

[155] *Id.*

[156] *Id.*

[157] *Id.*

[158] *Id.*

[159]

> "The Organisation for Economic Co-operation and Development has been called a think tank, monitoring agency, rich man's club, an unacademic university."
>
> "The OECD groups 30 member countries in an organisation that . . . provides governments a setting in which to discuss, develop and perfect economic and social policy. They compare experiences, seek answers to common problems and work to co-ordinate domestic and international policies that increasingly in today's globalised world must form a web of even practice across nations. Their exchanges may lead to agreements to act in a formal way - for example, by establishing legally-binding codes for free flow of capital and services, agreements to crack down on bribery or to end subsidies for shipbuilding. But more often, their discussion makes for better informed work within their own governments on the spectrum of public policy and clarifies the impact of national policies on the international community. And it offers a chance to reflect and exchange perspectives with other countries similar to their own."

What is OECD, ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, http://www.oecd.org/about/general/index.htm. "The original 20 members of the OECD are located in Western countries of Europe and North America. Next came Japan, Australia, New Zealand and Finland. More recently, Mexico, the Czech Republic, Hungary, Poland, Korea and the Slovak Republic have joined." *Membership*, http://www.oecd.org/about/general/member-countries.htm.

[160] The Council of Europe is an intergovernmental organisation which aims:

- to protect human rights, pluralist democracy and the rule of law;

Nations,[162] and Interpol[163] have played leading and important roles in building international awareness and cooperation in this regard.

- to promote awareness and encourage the development of Europe's cultural identity and diversity ;
- to seek solutions to problems facing European society (discrimination against minorities, xenophobia, intolerance, environmental protection, human cloning, Aids, drugs, organised crime, etc.);
- to help consolidate democratic stability in Europe by backing political, legislative and constitutional reform.

  The Council of Europe should not be confused with the European Union. The two organisations are quite distinct. The 15 European Union states, however, are all members of the Council of Europe.

An Overview, Council of Eur., http://www.coe.int/portal.asp?strScreenType=100&L=E&M=$t/1-1-1-1//portal.asp?L=E&M=$t/1-0-2-2/02/EMB,1,0,2,2,Overview.stm.

161

> The European Union (EU) was set up after the 2nd World War. The process of European integration was launched on 9 May 1950 when France officially proposed to create 'the first concrete foundation of a European federation'. Six countries (Belgium, Germany, France, Italy, Luxembourg and the Netherlands) joined from the very beginning. Today, after four waves of accessions (1973: Denmark, Ireland and the United Kingdom; 1981: Greece; 1986: Spain and Portugal; 1995: Austria, Finland and Sweden) the EU has 15 Member States and is preparing for the accession of 13 eastern and southern European countries.
>
> The European Union is based on the rule of law and democracy. It is neither a new State replacing existing ones nor is it comparable to other international organisations. Its Member States delegate sovereignty to common institutions representing the interests of the Union as a whole on questions of joint interest. All decisions and procedures are derived from the basic treaties ratified by the Member States.
>
> Principle objectives of the Union are:
>
> - Establish European citizenship (Fundamental rights; Freedom of movement; Civil and political rights);
> - Ensure freedom, security and justice (Cooperation in the field of Justice and Home Affairs);
> - Promote economic and social progress (Single market; Euro, the common currency; Job creation; Regional development; Environmental protection);
> - Assert Europe's role in the world (Common foreign and security; The European Union in the world).

The European Union at a glance, Europa, *at* http://europa.eu.int/abc-en.htm (last visited Apr. 17, 2002).

[162] *See, e.g., About the United Nations*, United Nations, http://www.un.org/aboutun/index.html (last visited Mar. 11, 2002).

[163] "Interpol exists to help create a safer world. Our aim is to provide a unique range of essential services for the law enforcement community to optimise the international effort to combat crime." *Vision*, Interpol, http://www.interpol.int/Public/Icpo/default.asp (last modified Mar. 11, 2002). One hundred seventy-nine countries are members of Interpol. *See Interpol Member States*, Interpol, http://www.interpol.int/Public/Icpo/Members/default.asp (last modified Apr. 17, 2002).

The first comprehensive inquiry into the criminal law problems of computer crime on the international scale was initiated by the (OECD). In 1983, a group of experts met and recommended that the OECD take the initiative in trying to achieve the harmonization of European computer crime legislation.[164] From 1983 to 1985, the OECD carried out a study of the possibility of an international application and harmonization of criminal laws to address cybercrime and abuse.[165] The study resulted in the 1986 report *Computer-related Crime: Analysis of Legal Policy*, which surveyed existing laws and proposals for reform and recommended a minimum list of abuses that countries should consider criminalizing.[166] This list was compiled as a result of a comparative analysis of substantive law around the world and outlined commonly recognized acts, which could constitute a shared basis for the different approaches taken by member states:

> (1) the input, alteration, erasure and/or suppression of computer data and/or computer programs made wilfully with the intent to commit an illegal transfer of funds or of another thing of value;
>
> (2) the input, alteration, erasure and/or suppression of computer data and/or computer programs made wilfully with the intent to commit a forgery;
>
> (3) the input, alteration, erasure and/or suppression of computer data and/or computer programs, or other interference with computer systems, made wilfully with the intent to hinder the functioning of a computer and/or of a telecommunication system;
>
> (4) the infringement of the exclusive right of the owner of a protected computer program with the intent to exploit commercially the program and put it on the market;
>
> (5) the access to or the interception of a computer and/or telecommunication system made knowingly and without the authorization of the person responsible for the system, either by infringement of security measures or for other dishonest or harmful intentions.[167]

From 1985 to 1989, the Select Committee of Experts on Computer-Related Crime of the Council of Europe discussed the issues raised by cybercrime and drafted Recommendation 89(9), adopted September 13, 1989.[168] Recommendation 89(9) emphasized the importance of an adequate and quick

---

[164] Schjolberg, *supra* note 164. *See also* SIEBER, *supra* note 134.

[165] *See* UNITED NATIONS MANUAL ON THE PREVENTION AND CONTROL OF COMPUTER-RELATED CRIME § II(C)(2) - ¶ 117, at 23 (1995), *at* http://www.uncjin.org/8th.pdf (May 10, 1999), http://www.uncjin.org/Documents/EighthCongress.html.

[166] *See id.* at § II(C)(2) - ¶ 117.

[167] *See id.* at § II(C)(2) - ¶ 118.

[168] *See* COUNCIL OF EUROPE, RECOMMENDATION NO. 4 (89) 9 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON COMPUTER RELATED CRIME, http://cm.coe.int/ta/rec/1989/89r9.htm (Sept. 13, 1989). *See also* UNITED NATIONS MANUAL ON THE PREVENTION AND CONTROL OF COMPUTER RELATED CRIME, *supra* note 165, at § II(C)(2) - ¶ 119.

> From 1985 to 1989 the Select Committee of Experts on Computer-Related Crime of the Council of Europe discussed the legal problems of computer crime. The Committee elaborated a report which was adopted by the European Committee on Crime Problems at its 38th Plenary Session in June 1989. The work of the Select Committee of Experts on Computer-Related Crime and of the European Committee on Crime Problems prepared Recommendation No. R (89), which was adopted on 13 September 1989 at the meeting of the Ministers' deputies.

response to cybercrime, the transborder nature of which requires harmonization of law and practice and improved international legal cooperation.[169] It further emphasized the need for international consensus in criminalizing and addressing certain computer-related offenses.[170] The Recommendation featured a "minimum list" of crimes to be prohibited and prosecuted by international consensus, as well as an "optional list" that describes prominent offenses on which international consensus would be difficult to reach.[171] The "minimum list" includes:

> "Computer Fraud": The input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing, that influences the result of data processing thereby causing economic or possessory loss of property of another person with the intent of procuring an unlawful economic gain for himself or for another person;

SIEBER, *supra* note 134, at 161
(footnotes omitted).

[169] *See* COUNCIL OF EUROPE, RECOMMENDATION NO. 4, *supra* note 168. *See also* UNITED NATIONS MANUAL ON THE PREVENTION AND CONTROL OF COMPUTER RELATED CRIME, *supra* note 165, at § II(C)(2) - ¶ 120 at 23-24.

[170] *See* COUNCIL OF EUROPE, RECOMMENDATION NO.4, *supra* note 168:

> The Committee of Ministers, . . .
>
> Recognising the importance of an adequate and quick response to the new challenge of computer-related crime;
>
> Considering that computer-related crime often has a transfrontier character;
>
> Aware of the resulting need for further harmonisation of the law and practice and of improving international legal co-operation,
>
> Recommends the governments of member States to:
>
> 1. Take into account, when reviewing their legislation or initiating new legislation, the report on computer-related crime elaborated by the European Committee on Crime Problems, and in particular the so-called guidelines for the national legislatures;
>
> 2. Report to the Secretary General of the Council of Europe during 1993, of any developments in their legislation, judicial practice and experiences of international legal co-operation in respect of computer-related crime.

See also UNITED NATIONS MANUAL ON THE PREVENTION AND CONTROL OF COMPUTER RELATED CRIME, *supra* note 165, at § II(C)(2) - ¶ 120, at 23 (explaining that the recommendation suggested that governments "take into account, when reviewing their legislation or initiating new legislation, the report on computer-related crime. . . and in particular the guidelines for the national legislatures").

[171] *See* UNITED NATIONS MANUAL ON THE PREVENTION AND CONTROL OF COMPUTER RELATED CRIME, *supra* note 165, at § II(C)(2) - ¶ 120 at 23-24("The guidelines for national legislatures include a minimum list, which reflects the general consensus of the Committee regarding certain computer-related abuses that should be dealt with by criminal law, as well as an optional list, which describes acts that have already been penalized in some States, but on which an international consensus for criminalization could not be reached").

> "Computer Forgery": The input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing, in a manner or under such conditions, as prescribed by national law, that it would constitute the offense of forgery if it had been committed with respect to a traditional object of such an offense;
>
> "Damage to Computer Data or Computer Programs": The erasure, damaging, deterioration or suppression of computer data or computer programs without right;
>
> "Computer Sabotage": The input, alteration, erasure or suppression of computer data or computer programs, or other interference with computer systems, with the intent to hinder the functioning of a computer or a telecommunication system;
>
> "Unauthorised Access": The access without right to a computer system or network by infringing security measures;
>
> "Unauthorised Interception": The interception, made without right and by technical means, of communications to, from and within a computer system or network;
>
> "Unauthorised Reproduction of a Protected Computer Program": The reproduction, distribution or communication to the public without right of a computer program which is protected by law;
>
> "Unauthorized Reproduction of a Topography": The reproduction without right of a topography protected by law, of a semi-conductor product, or the commercial exploitation or the importation for that purpose, done without right, of a topography or of a semi-conductor product manufactured by using the topography.[172]

The optional list involves:

> "Alteration of Computer Data or Computer Programs": The alteration of computer data or computer programs without right;
>
> "Computer Espionage": The acquisition by improper means or the disclosure, transfer or use of a trade or commercial secret without right or any other legal justification, with intent either to cause economic loss to the person entitled to the secret or to obtain an unlawful economic advantage for oneself or a third person;
>
> "Unauthorised Use of a Computer": The use of a computer system or network without right, that either: (a) is made with the acceptance of a significant risk of loss being caused to the person entitled to use the system or harm to the system or its functioning, or (b) is made with the intent to cause loss to the person entitled to use the system or harm to the system or its functioning, or (c) causes loss to the person entitled to use the system or harm to the system or its functioning;
>
> "Unauthorised Use of a Protected Computer Program": The use without right of a computer program which is protected by law and which has been reproduced without right, with the intent, either to procure an unlawful economic gain for himself or for another person or to cause harm to the holder of the right."[173]

In 1990, the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders addressed the legal problems posed by cybercrime.[174] The Congress produced a resolution calling for Member States to intensify their efforts to combat computer crime by modernizing their national criminal laws and procedures, improving computer security and prevention measures, and

---

[172] *See id*. at § II(C)(2) - ¶ 121, at 24.

[173] *See id*.

[174] *See, e.g.,* SIEBER, *supra* note 134, at 162 (noting that cybercrime was discussed at Eighth UN Congress and at "the accompanying Symposium on the Prevention and Prosecution of Computer Crime, organised by the Foundation for Responsible Computing").

promoting the development of a comprehensive international framework of guidelines and standards for preventing, prosecuting, and punishing computer-related crime in the future.[175] Most notably, the resolution called for Member States to intensify their efforts toward the modernisation of national criminal laws and procedures, including measures to:

> (a) Ensure that existing offences and laws concerning investigative powers and admissibility of evidence in judicial proceedings adequately apply and, if necessary, make appropriate changes;
>
> (b) In the absence of laws that adequately apply, create offences and investigative and evidentiary procedures, where necessary, to deal with this novel and sophisticated form of criminal activity;
>
> (c) Provide for the forfeiture or restitution of illegally acquired assets resulting from the commission of computer-related crimes.[176]

In 1990, the Third Committee of the United Nations General Assembly drafted a resolution inviting governments to be guided by the resolutions adopted at the Eighth United Nations Congress in "the formulation of appropriate legislation and policy directives."[177] The General Assembly adopted this resolution on December 14, 1990.[178]

In 1992, the Council of the OECD and 24 of its Member countries adopted the Recommendation of the Council Concerning Guidelines for the Security of Information Systems, intended to provide a foundational information security framework for the public and private sectors.[179] The *Guidelines for the Security of Information Systems* [hereinafter, "*Guidelines*"] were annexed to the Recommendation.[180] This framework includes laws, codes of conduct, technical measures, management and user practices, and public education provisions.[181] The *Guidelines* focus on the implementation of minimum standards for the security of information systems.[182] In parallel, however, the *Guidelines* request that Member States

---

[175] *See, e.g., id*. at 162-163 (citing *8th U.N. Congress on the Prevention of Crime and the Treatment of Offenders*, U.N., U.N. Doc. A/CONF. 144/L.11 (1990)).

[176] *See id.* at 162.

[177] *See id.* at 163 (quoting *Crime Prevention and Criminal Justice Report of the 3d Comm.*, U.N. GAOR, at 123, U.N. Doc. A/45/756 (1990)).

[178] *See, e.g., id.*

[179] *See* ORG. FOR ECON. CO-OPERATION AND DEV., RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES FOR THE SECURITY OF INFO. SYSTEMS, at http://www.oecd.org/dsti/sti/it/secur/index.htm (Nov. 26, 1992). *See also* SIEBER, *supra* note 134, at 158.

[180] *See* RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES FOR THE SECURITY OF INFO. SYSTEMS, *supra* note 179.

[181] *See* ORG. FOR ECON. CO-OPERATION AND DEV., GUIDELINES FOR THE SECURITY OF INFO. SYSTEMS, *supra* note 179.

[182] *See id.*

establish adequate penal, administrative or other sanctions for misuse of information systems, and develop means for mutual assistance, extradition and other international cooperation in matters of security of information systems.[183]

In 1995 the *United Nations Manual on the Prevention and Control of Computer-Related Crime* was published.[184] The *Manual* examines the phenomenon of computer crime, substantive criminal law protecting the holder of data and information, substantive criminal law protecting privacy, procedural law, crime prevention in the computer environment, and the need for and avenues to international cooperation.[185]

In 1995, Interpol held its first international conference on computer crime.[186] The conference confirmed a high level of concern in the law enforcement community over the propagation of computer crime; Conference participants were especially troubled by the lack of a worldwide mechanism to address such crime effectively and efficiently.[187] Interpol held subsequent conferences on computer crime in 1995, 1996, 1998 and 2000.[188] Interpol's approach to cybercrime has been to harness

> the expertise of its members in the field of Information Technology Crime (ITC) through the vehicle of a 'working party' or a group of experts. In this instance, the working party consists of the Heads or experienced members of national computer crime units. These working parties have been designed to reflect regional expertise and exist in Europe, Asia, the Americas and in Africa. All working parties are in different stages of development.[189]

---

[183] *See id. See also* SIEBER, *supra* note 134, at 158.

[184] *See* U.N. MANUAL ON THE PREVENTION AND CONTROL OF COMPUTER-RELATED CRIME, *supra* note 165.

[185] *See id*.

[186] *See, e.g.,* SIEBER, *supra* note 134, at 188-89. In 1981, Interpol held its First Interpol Training Seminar for Investigators of Computer Crime. *See, e.g.,* Schjolberg, *supra* note 164.

[187] *See* Interpol, Steering Committee for Information Technology Crime, http://www.interpol.int/Public/TechnologyCrime/WorkingParties/Default.asp#steeringCom:

> The Steering Committee (SC) was formed to co-ordinate and harmonise the various regional working party initiatives. It is represented by the Chairperson, Vice-Chairperson and a third member from each regional WP and is co-ordinated by the representative from the General Secretariat. The idea was to streamline the individual efforts of the member countries by avoiding unnecessary duplication and the resultant waste of human and financial resources. The SC has now gone a step further by contacting organisations outside of Interpol and involving them in our initiatives…to date we have thus achieved success most notably with the High Tech Crime Sub-group of the G8, the International Chamber of Commerce, UNAFEI (the United Nations Asia Institute for the Prevention of Crime and the Treatment of Offenders), as well as with several academic institutions.

[188] *See, e.g.,* Schjolberg, *supra* note 164.

[189] *Interpol's Contribution to Combating Information Technology Crime*, INTERPOL, *at* http://www.interpol.int/Public/TechnologyCrime/default.asp (last modified Mar. 11, 2002).

The first Interpol working party, the European Working Party on Information Technology Crime, was established in 1990;[190] the other three working parties were established later.[191] Interpol has also established a Steering Committee for Information Technology Crime, which coordinates and harmonizes the initiatives of the various working parties.[192]

In 1995, the Council of Europe adopted Recommendation No. R (95)13 of the Committee of Ministers to Member states, spelling out the principles that should guide states and their investigating authorities in the field of information technology.[193] The principles cover search and seizure, technical surveillance, obligations to co-operate with the investigating authorities, electronic evidence, use of encryption, research, statistics and training, and international cooperation.[194] The document addresses these issues from the perspectives of investigating both cybercrime and traditional crimes where evidence may be found or transmitted in electronic form.[195]

In 1996 and 1997, the European Commission issued several documents dealing with harmful and illegal content online and with the safe use of the Internet.[196] On April 24, 1997, the European Parliament adopted a resolution on the European Commission's "communication on illegal and harmful content on the Internet, supporting the initiatives undertaken by the Commission and stressing the need for

---

[190] *European Working Party on Information Technology Crime*, INTERPOL, *at* http://www.interpol.int/Public/TechnologyCrime/default.asp (last modified Mar. 11, 2002).

[191] *See Regional Working Parties*, INTERPOL, *at* http://www.interpol.int/Public/TechnologyCrime/WorkingParties/Default.asp#europa (last modified Mar. 11, 2002).

[192] *See Steering Committee for Information Technology Crime*, INTERPOL, *at* http://www.interpol.int/Public/TechnologyCrime/WorkingParties/Default.asp#europa (last modified Mar. 11, 2002).

[193] *See Comm. of Ministers*, Eur. Parl. Ass., Recommendation No. R (95) 13 of the Comm. of Ministers to Member States, *at* http://www.privacy.org/pi/intl_orgs/coe/info_tech_1995.html (Sept. 11, 1995). *See also* SIEBER, *supra* note 134, at 179.

[194] *See Comm. of Ministers*, *supra* note 193. *See also* SIEBER, *supra* note 134, at 179-181.

[195] *Id.*

[196] *See, e.g.,* SIEBER, *supra* note 134, at 172-173.

> The Communication on illegal and harmful content . . . confirms that all persons involved in the Internet . . . are subject to the respective laws of the Member States and do not operate in a legal vacuum. The paper identifies different variations of illegal and harmful content and gives policy option for EU action. . . .
>
> The Green Paper on the Protection of Minors and Human Dignity. . . . deals with . . . the fight against the dissemination of content offensive to human dignity and the protection of minors against exposure to content that is harmful to their development. The Green Paper proposes ten basic questions to help create the conditions for the establishment of a coherent framework for the protection of minors and human dignity. . . .
>
> In the Action Plan on promoting safe use of the Internet, the Commission identified areas where concrete measures are needed and where Community resources should be made available in order to encourage an environment favourable to the development of the Internet industry. These areas are the promotion of self-regulation and creation of content-monitoring schemes including an European network of hot-lines, the demonstration and application of effective filtering services and compatible rating systems, and the promotion of awareness actions directed at users, in particular children, parents and teachers. . . .

international co-operation in various areas, to be initiated by the Commission."[197] And in April of 1998 the European Commission presented the European Council with a report on computer-related crime for which it had contracted.[198]

In 1997, the Justice and Interior Ministers of the Group of Eight[199] (G8) met in Washington and adopted ten Principles to Combat High-Tech Crime:

I. There must be no safe havens for those who abuse information technologies.
II. Investigation and prosecution of international high-tech crimes must be coordinated among all concerned States, regardless of where harm has occurred.
III. Law enforcement personnel must be trained and equipped to address high-tech crimes.
IV. Legal systems must protect the confidentiality, integrity, and availability of data and systems from unauthorized impairment and ensure that serious abuse is penalized.
V. Legal systems should permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime.
VI. Mutual assistance regimes must ensure the timely gathering and exchange of evidence in cases involving international high-tech crime.
VII. Transborder electronic access by law enforcement to publicly available (open source) information does not require authorization from the State where the data resides.
VIII. Forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions must be developed and employed.
IX. To the extent practicable, information and telecommunications systems should be designed to help prevent and detect network abuse, and should also facilitate the tracing of criminals and the collection of evidence.
X. Work in this area should be coordinated with the work of other relevant international fora to ensure against duplication of efforts.[200]

The Ministers also adopted the Action Plan to Combat High-Tech Crime in which, among other things, they pledged to "[r]eview our legal systems to ensure that they appropriately criminalize abuses of telecommunications and computer systems and to promote the investigation of high-tech crimes."[201]

In 1997, the OECD Directorate for Science, Technology and Industry directed a five-year review of the progress that had been made toward implementing the 1992 *Guidelines for the Security of Information Systems*, discussed above.[202] The review was conducted by means of a questionnaire issued

---

[197] *Id*. at 174.

[198] *Creating a Safer Information Society, supra* note 29, at iv (2000). The European Commission awarded the contract for the study to the University of Würzburg on October 11, 1996; the study was completed in 1998. *See* SIEBER, *supra* note 134.

[199] United States of America, United Kingdom, France, Germany, Canada, Japan, Italy and Russia.

[200] Meeting of the Justice and Interior Ministers of The Eight, December 9-10, 1997, COMMUNIQUE ANNEX, WASHINGTON, D.C., http://www.cybercrime.gov/principles.htm.

[201] Action Plan to Combat High-Tech Crime, Item #3, Meeting of the Justice and Interior Ministers of The Eight, December 9-10, 1997, COMMUNIQUE ANNEX, WASHINGTON, D.C., http://www.cybercrime.gov/action.htm.

[202] *See* OECD, DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY – COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY, REVIEW OF THE 1992 GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS (1997), http://www.oecd.org/dsti/sti/it/secur/index.htm. *See also* OECD, RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES FOR THE SECURITY OF INFO.

to OECD Member countries.[203] The review disclosed, among other things, that the responding countries had experienced difficulties in developing laws and procedures relating to information security because of "differences in the various legal systems and how they deal with security matters . . . such as . . . computer crimes."[204] The general consensus was that the *Guidelines* were still adequate and did not need to be revised.[205]

Also in 1997, the Council of Europe's European Committee on Crime Problems (CDPC) created a new Committee of Experts on Crime in CyberSpace (PC-CY).[206] The Committee of Experts on Crime in Cyberspace was assigned to examine -- "in light of Recommendations No R (89) 9 . . . and No R (95) 13"[207] -- the problems "of criminal procedural law connected with information technology" including, *inter alia*, "cyberspace offences" and "other substantive criminal law issues where a common approach may be necessary for the purposes of international co-operation". [208]

SYSTEMS, *supra* note 179. The Recommendation suggested that the *Guidelines* be reviewed every five years "with a view to improving international co-operation on issues relating to the security of information systems."

[203]OECD, DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY, *supra* note 202.

[204] *Id.* at 10.

[205] *See id.* at 18.

[206]*See* COUNCIL OF EUROPE, 583RD MEETING OF THE MINISTERS' DEPUTIES, 4 FEBRUARY 1997, Appendix 13, http://www.cm.coe.int/dec/1997/583/583.a13.html. *See* SIEBER, *supra* note 134, at 181.

[207]COUNCIL OF EUROPE, 583RD MEETING OF THE MINISTERS' DEPUTIES, *supra* note 206, at Appendix 13 § 4(c).

[208] SIEBER, *supra* note 134. *See* COUNCIL OF EUROPE, 583RD MEETING OF THE MINISTERS' DEPUTIES, *supra* note 206, at Appendix 13 § 4(c):

> The Committee's terms of reference are as follows:
>
> Examine . . . in particular the following subjects:
>
> i) cyber-space offences, in particular those committed through the use of telecommunication networks, e.g. the Internet, such as illegal money transactions, offering illegal services, violation of copyright, as well as those which violate human dignity and the protection of minors;
>
> ii) other substantive criminal law issues where a common approach may be necessary for the purposes of international co-operation such as definitions, sanctions and responsibility of the actors in cyber-space, including Internet service providers;
>
> iii) the use, including the possibility of transborder use, and the applicability of coercive powers in a technological environment, e.g. interception of telecommunications and electronic surveillance of information networks, . . . taking into account the problems caused by particular measures of information security, e.g. encryption ;
>
> iv) the question of jurisdiction in relation to information technology offences, e.g. to determine the place where the offence was committed (*locus delicti*) and which law should accordingly apply, including . . . the question how to solve positive jurisdiction conflicts and how to avoid negative jurisdiction conflicts;

The new Committee was also given the task of drafting "a binding legal instrument" dealing with these issues. [209]

The Council of Europe's Committee of Experts on Crime in Cyber-Space took this assignment to heart, preparing a Convention on Cyber-Crime.[210] The preparation of the Convention was a long process, taking four years and twenty-seven drafts before the final version, dated May 25, 2001, was submitted to the European Committee on Crime Problems at its 50th Plenary Session, June 18-22, 2001.[211] The final version contained a Preamble and four Chapters.[212]

Chapter II of the Draft Convention on Cyber-Crime contains the provisions relevant to the issues considered in this article. Chapter II, measures to be taken at the national level," is divided into Section 1, "substantive criminal law" and Section 2, "procedural law."[213] The Explanatory Memorandum accompanying the Draft Convention indicates that Section 1 seeks to:

> improve the means to prevent and suppress computer- or computer – related crime by establishing a common minimum standard of relevant offences. This kind of harmonisation alleviates the fight against such crimes on the national and on the international level as well. Correspondence in domestic law may prevent abuses from being shifted to a Party with a previous lower standard. As a consequence, the exchange of useful common experiences in the practical handling of cases may be enhanced, too. International cooperation (esp. extradition and mutual legal assistance) is facilitated e.g. regarding requirements of double criminality.[214]

Parties to the Convention would agree to adopt legislation and other measures necessary to establish certain activities as cybercrimes under domestic law.[215] The activities are set out in five titles to Chapter II: (1) illegal interception of and/or interference with computer data, illegal access to and/or interference

---

> v) questions of international co-operation in the investigation of cyber-space offences, in close co-operation with the Committee of Experts on the Operation of European Conventions in the Penal Field (PC-OC).
>
> The Committee should draft a binding legal instrument, as far as possible, on the items i) - v), with particular emphasis on international questions and, if appropriate, accessory recommendations regarding specific issues. The Committee may make suggestions on other issues in the light of technological developments.

[209] COUNCIL OF EUROPE, 583RD MEETING OF THE MINISTERS' DEPUTIES, *supra* note 206, at Appendix 13 § 4(c).

[210] *See, e.g.,* COUNCIL OF EUROPE, COMMITTEE OF EXPERTS ON CRIME IN CYBER-SPACE, FINAL ACTIVITY REPORT (May 25, 2001), http://conventions.coe.int/Treaty/EN/cadreprojets.htm [hereinafter FINAL ACTIVITY REPORT].

[211] *See* EXPLANATORY MEMORANDUM, supra note 95, at ¶¶ 7-15.

[212] *See* FINAL ACTIVITY REPORT, *supra* note 210.

[213] *Id.* at Chapter I - ¶ 33.

[214] *See* EXPLANATORY MEMORANDUM, *supra* note 95, at ¶¶ 7-15.

[215] *See, e.g.,* FINAL ACTIVITY REPORT, *supra* note 210, at DRAFT CONVENTION ON CYBER-CRIME § 1.

with computer systems, and the misuse of devices to commit any of these offenses;[216] (2) computer-related forgery and fraud; [217] (3) child pornography;[218] (4) the infringement of copyright and related

---

[216] *See* EXPLANATORY MEMORANDUM, *supra* note 95, at ¶ 35:

> Title 1 includes the core of computer-related offences, offences against the confidentiality, integrity and availability of computer data and systems, representing the basic threats, as identified in the discussions on computer and data security to which electronic data processing and communicating systems are exposed. The heading describes the type of crimes which are covered, that is the unauthorised access to and illicit tampering with systems, programmes or data.

See also FINAL ACTIVITY REPORT, *supra* note 210, at § 1, title 1:

> *Article 2 - Illegal access*
>
> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.
>
> *Article 3 - Illegal interception*
>
> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent**,** or in relation to a computer system that is connected to another computer system.
>
> *Article 4 - Data interference*
>
> 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
>
> 2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.
>
> *Article 5 - System interference*
>
> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.
>
> *Article 6 – Misuse of devices*
>
> 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:
>
> a. the production, sale, procurement for use, import, distribution or otherwise making available of:

i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b. the possession of an item referred to in paragraphs (a)(i) or (ii) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1(a)(ii).

[217] *See* EXPLANATORY MEMORANDUM, *supra* note 95, at ¶ 35:

> Titles 2 – 4 include other types of 'computer-related offences', which play a greater role in practice and where computer and telecommunication systems are used as a means to attack certain legal interests which mostly are protected already by criminal law against attacks using traditional means. The Title 2 offences (computer-related fraud and forgery) have been added by following suggestions in the guidelines of the Council of Europe Recommendation No. R (89) 9.

See also FINAL ACTIVITY REPORT, *supra* note 210, at § 1, title 2:

> *Article 7 – Computer-related forgery*
>
> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.
>
> *Article 8 – Computer-related fraud*
>
> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another by:
>
> a. any input, alteration, deletion or suppression of computer data,
>
> b. any interference with the functioning of a computer or system,
>
> with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another.

rights;[219] and (5) provisions governing the imposition of aiding and abetting and corporate liability.[220] Parties also agree to establish "effective, proportionate and dissuasive criminal . . . sanctions" for the

---

[218] *See* EXPLANATORY MEMORANDUM, *supra* note 95, at ¶ 35:

> Title 3 covers the 'content-related offences of unlawful production or distribution of child pornography by use of computer systems as one of the most dangerous *modi operandi* in recent times. The committee drafting the Convention discussed the possibility of including other content-related offences, such as the distribution of racist propaganda through computer systems. However, the committee was not in a position to reach consensus on the criminalisation of such conduct. While there was significant support in favour of including this as a criminal offence, some delegations expressed strong concern about including such a provision on freedom of expression grounds. Noting the complexity of the issue, it was decided that the committee would refer to the European Committee on Crime Problems (CDPC) the issue of drawing up an additional Protocol to the present Convention.

See also FINAL ACTIVITY REPORT, *supra* note 210, at § 1, title 3:

> *Article 9 – Offences related to child pornography*
>
> 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
>
> > a. producing child pornography for the purpose of its distribution through a computer system;
> >
> > b. offering or making available child pornography through a computer system;
> >
> > c. distributing or transmitting child pornography through a computer system;
> >
> > d. procuring child pornography through a computer system for oneself or for another;
> >
> > e. possessing child pornography in a computer system or on a computer-data storage medium.
>
> 2. For the purpose of paragraph 1 above "child pornography" shall include pornographic material that visually depicts:
>
> > a. a minor engaged in sexually explicit conduct;
> >
> > b. a person appearing to be a minor engaged in sexually explicit conduct;
> >
> > c. realistic images representing a minor engaged in sexually explicit conduct.
>
> 3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.
>
> 4. Each Party may reserve the right not to apply, in whole or in part, subparagraphs 1(d), 1(e), 2(b) and 2(c).

[219] *See* EXPLANATORY MEMORANDUM, *supra* note 95, at ¶ 35:

> Title 4 sets out 'offences related to infringements of copyright and related rights'. This was included in the Convention because copyright infringements are one of the most widespread forms of computer- or computer-related crime and its escalation is causing international concern.

See also FINAL ACTIVITY REPORT, *supra* note 210, at § 1, title 4:

> *Article 10 - Offences related to infringements of copyright and related rights*
>
> 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 of the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such Conventions, where such acts are committed wilfully, [at least] (4) on a commercial scale and by means of a computer system.
>
> 2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations done in Rome (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such Conventions, where such acts are committed wilfully, [at least] (5) on a commercial scale and by means of a computer system.
>
> 3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

[220] *See* FINAL ACTIVITY REPORT, *supra* note 210, at Chapter I - ¶ 33; EXPLANATORY MEMORANDUM, *supra* note 95, at ¶ 35 ("Title 5 includes additional provisions on attempt, aiding and abetting and sanctions and measures, and, in compliance with recent international instruments, on corporate liability"). *See also* FINAL ACTIVITY REPORT, *supra* note 210, at § 1, title 5:

> *Article 11 - Attempt and aiding or abetting*
>
> 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.
>
> 2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, 9 (1) a and 9 (1) c of this Convention.
>
> 3. Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.
>
> *Article 12 – Corporate liability*
>
> 1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that a legal person can be held liable for a criminal offence established in accordance with this Convention, committed for its benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on:

commission of any of the specified offenses.[221] The Parliamentary Assembly of the Council of Europe approved the Draft Convention on Cyber Crime at its April, 2001 session,[222] and it was opened for signature by the member states on November 23, 2001.[223]

In May of 2000, the G8 held a cybercrime conference to discuss "how to jointly crack down on Internet crime."[224] The conference, which brought together "about 300 judges, police, diplomats and business leaders from the G8 states -- the United States, Japan, Germany, Britain, France, Italy, Canada and Russia,[225] drafted an agenda for a follow-up summit to be held in July.[226] At the July, 2000 summit, the G8 issued a communiqué which declared, in pertinent part, that it would "take a concerted approach to high-tech crime, such as cyber-crime, which could seriously threaten security and confidence in the global information society."[227] The communiqué noted that the G8's approach to these matters was set out in paragraph eight of the Okinawa Charter on Global Information Society:

> International efforts to develop a global information society must be accompanied by co-ordinated action to foster a crime-free and secure cyberspace. We must ensure that effective measures, as set

---

> a. a power of representation of the legal person;
>
> b. an authority to take decisions on behalf of the legal person;
>
> c. an authority to exercise control within the legal person.
>
> 2. In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.
>
> 3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.
>
> 4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

[221] FINAL ACTIVITY REPORT, *supra* note 210, at § 1, title 5, Article 13.

[222] *See The Parliamentary Assembly – Reactions and Conclusions*, Council of Europe, http://press.coe.int/press2/press.asp?B=54,0,0,107,0&M=http://press.coe.int/dossiers/107/E/e-ap.htm/

[223] *See* COUNCIL OF EUROPE, CONVENTION ON CYBERCRIME (November 23, 2001), http://conventions.coe.int/Treaty/EN/cadreprincipal.htm.

[224] *Group of Eight Meets to Discuss International Cooperation on Cybercrime*, ADLAW BY REQUEST, May 22, 2000, http://adlawbyrequest.com/international/G8Cybercrime.shtml.

[225] *Blueprint to Fight Cybercrime*, WIRED NEWS, May 15, 2000, http://www.wired.com/news/print/0,1294,36332,00.html.

[226] *Group of Eight Meets to Discuss International Cooperation on Cybercrime*, *supra* note 224; *G8 Hems and Haws on Cybercrime*, WIRED NEWS, May 17, 2000, http://www.wired.com/news/politics/0,1283,36398,00.html.

[227] G8 COMMUNIQUE OKINAWA 2000 ¶ 44 (July 23, 2000), http://www.g7.utoronto.ca/g7/summit/2000okinawa/finalcom.htm.

> out in the OECD Guidelines for Security of Information Systems, are put in place to fight cyber-crime. G8 co-operation within the framework of the Lyon Group on Transnational Organised Crime will be enhanced. We will further promote dialogue with industry. . . . Urgent security issues such as hacking and viruses also require effective policy responses. We will continue to engage industry and other stakeholders to protect critical information infrastructures.[228]

The G8 also pledged to establish a "Digital Opportunity Taskforce" which would explore how to integrate the efforts of the G8 members into "a broader international approach."[229] The Taskforce held meetings during the late 2000 and early 2001 and submitted a report containing their Proposed Plan of Action to the personal representatives of the G8 leaders in May, 2001.[230] The report did not address cybercrime, but focused instead on the need to overcome the "digital divide."[231]

In June of 2000, an Action Plan prepared by the European Commission and the European Council was adopted by the Feira Summit of the European Council.[232] Among other things, the Action Plan called for the "establishment of a co-ordinated and coherent approach to cybercrime by the end of 2002."[233] A Commission report issued subsequently explained that "an EU legislative instrument approximating substantive criminal law in the field of computer-related crime has been on the EU agenda" since October, 1999.[234] The report noted that the "Commission has followed the work of the Council of Europe on" the Draft Convention on Cyber-Crime discussed above.[235] It also explained that the European Union's planned approximation on substantive cybercrime law "could go further than the C.o.E Convention, which will represent a minimum of international cooperation", could "be operational within a shorter period of time" and "would bring computer crime within the realms of EU law and introduce EU law enforcement mechanisms."[236] This portion of the report then goes on to announce four measures the European Commission plans to take:

> 1) introduce a proposal for a Council Framework Decision that will include provisions for the approximation of laws on child pornography on the Internet, laws that go further than the measures contemplated by the Council of Europe's Draft Convention on Cyber-crime;[237]

---

[228] G8 OKINAWA CHARTER ON GLOBAL INFORMATION SOCIETY ¶ 8 (July 22, 2000), http://www.g7.utoronto.ca/g7/summit/2000okinawa/gis.htm.

[229] *Id*. at ¶ 18 (July 22, 2000).

[230] *See* G8 DIGITAL OPPORTUNITY TASKFORCE, THE CURRENT STATE AND PERSPECTIVE OF THE DIGITAL OPPORTUNITY TASKFORCE (June 1, 2001), http://www.mofa.go.jp/policy/economy/it/df0106.html.

[231] *See id.*

[232] *See Creating a Safer Information Society, supra* note 29, at § 1.

[233] *Id.*

[234] *Id.* at § 4

[235] *Id.*

[236] *Id.*

[237] *Id. See also id.* at § 7.1 (statement of legislative proposals).

2) bring forward a proposal to approximate high tech offenses, notably "hacking and denial of service attacks", which will include standard definitions and "go further than the draft Council of Europe Convention by ensuring that serious cases of hacking and denial of service attacks are punishable by a minimum penalty in all Member States";[238]

3) "examine the scope for action against racism and xenophobia on the Internet with a view to bringing forward a proposal for a Council Framework Decision . . . covering both off-line and on-line racist and xenophobic activity";[239]

4) consider "how to improve the effectiveness of efforts against the illicit drugs trade on the Internet."[240]

4. CUMULATIVE BENEFITS

Cumulatively, national efforts and those of international organizations have reinforced each other, achieving nearly global attention to the problems of cybercrime and terrorism, and promoting international harmonization of legal approaches.[241] National efforts at combating cybercrime encompass different levels of sophistication and priority, but are present in at least 40 major countries (which actively shape international law and order). These countries represent all parts of the world and run the gamut of advanced, industrialized and developing nations. Many countries are developing specialized police capabilities through equipment, training and laws.

International and supranational organizations have significantly contributed to the harmonization of criminal law as well as of underlying civil and administrative law in all of the areas of computer-related criminal law reform. Ulrich Sieber, author of the cybercrime study commissioned by the European Commission,[242] found a close interrelationship between law reform at the national level and activities on the international and supranational level. As Sieber explained, "the preparation of the respective initiatives had a considerable impact on national laws by bringing the major national players together."[243] The European Community's power to adopt binding directives opened a new age of legal harmony in Europe, and the process continues.[244] Similar efforts are taking place in other parts of the world.

But even as these efforts progress, global cybercrime law continues to be a patchwork of new laws, old laws and no laws. Experts emphasize the persistent need for the development of comprehensive, consistent national legal frameworks that can be integrated into a global cybercrime

---

[238] *Id.*

[239] *Id.* As was noted above, the Committee drafting the Council of Europe's Convention on Cyber-Crime did not include provisions addressing the online dissemination of racist and other hate speech. *See* notes 417 & 418, *infra.*.

[240] *Id.* This, of course, is something that is not addressed in the Council of Europe's Draft Convention on Cyber-Crime.

[241] *See, e.g.,* SIEBER, *supra* note 134, at 33.

[242] *See* § III(A)(3), *supra*. For the results of the study, see SIEBER, *supra* note 134.

[243] SIEBER, *supra* note 134, at 34.

[244] *See* § III(A)(3), *supra*.

strategy;[245] as Section I demonstrated, the existence of such laws is a fundamental prerequisite for investigation, as well as for prosecution. The section below examines the approach that is being taken to developing these legal frameworks and its likelihood of success.

B. CONSENSUS CRIMES: FOUNDATION OF A GLOBAL STRATEGY

> *When one country's laws criminalize . . . computer-related crime and another country's laws do not, cooperation to solve a crime, as well as the possibility of extraditing the criminal to stand trial, may not be possible. Inadequate regimes . . . can . . . shield criminals from law enforcement: criminals can go unpunished in one country, while they thwart the efforts of other countries to protect their citizens.* [246]

Inconsistent national criminal laws were acceptable so long as crime was parochial.[247] A nation's decision whether to criminalize activities was a matter solely within national discretion because the consequences of that decision would impact only upon those living within its borders, generally its own citizens. Three hundred years ago, for example, a French citizen's chances of ever finding himself in China were remote, to say the least. But as earthbound technology - ocean-going vessels, trains, automobiles and then planes - evolved, citizens of one nation were increasingly likely to find themselves in another country's jurisdiction.

This trend accelerated and took new forms with the proliferation of computer technology, which makes geographical borders irrelevant; with the Internet people can now cross borders digitally without a passport, getting on a plane, or ever leaving their bedroom. In fact, through the looping and weaving nature of computer routers and the WWW, someone can intend to visit a Web site in France (only) but never realize that his or her communication is being routed through Japan and Brazil to get there. This is a major departure from the previous state of affairs.

While the world has slowly begun to deal with traditional border crossings, the nature of cyberspace is highly inconsistent with terrestrial based jurisprudence. Cyber-criminals can hopscotch around the world, exploiting gaps in criminal laws and committing depredations with essential impunity and citizens abiding by the laws of their own country can find themselves subject to prosecution in another country under its different laws.[248] The conflict in laws can lead to peculiar results: if, for

---

[245] See, e.g., *Conclusions of the Study on Effective Measures to Prevent and Control High-Technology and Computer-Related Crime*, *supra* note 30, item 4 at 13 ("[M]any experts are of the view that nothing less than a comprehensive, global legal instrument against high-technology and computer-related crime will be sufficient to establish the policies, powers, procedures and mechanisms for international cooperation needed to deal effectively with transnational computer-related crime").

[246] PRESIDENT'S WORKING GROUP ON UNLAWFUL CONDUCT ON THE INTERNET,THE ELECTRONIC FRONTIER: THE CHALLENGE OF UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET 41 (2000), http://www.usdoj.gov/criminal/cybercrime/unlawful.pdf.

[247] *See* § II(B), *supra*.

[248] *See, e.g.,* League Against Racism and Antisemitism v. Yahoo!, Inc., No. RG: 00/05308 (County Ct. of Paris, Nov. 2000), http://www.kentlaw.edu/perritt/conflicts/yahooparis.html. *See also* John F. McGuire, Note, *When Speech Is Heard Around the World: Internet Content Regulation in the United States and Germany,* 74 N.Y.U. L. REV. 750, 768-770 (1999), *available at* http://www.nyu.edu/pages/lawreview/74/3/McGuire.pdf (German prosecutors charged CompuServe executive as an accessory to the dissemination of pornography and extremist propaganda based on content of online news groups); Nancy Finken, *Nebraska's Nazi*, Nebraska Public Radio,

example, CompuServe were to take down a Nazi web site because of its content (not because of any violation of CompuServe's terms of service), CompuServe could find itself being sued in the United States for violating the site operators' First Amendment rights, whereas if it did not take down the web site legal action could be brought against it in France and/or Germany, for keeping the site up.

The emergence of cybercrime in its networked and interconnected nature makes it imperative to achieve transnational consistency in criminal prohibitions. One way to accomplish this would be to create a single code of law governing the commission of cybercrime (which would have to be an agreed-upon term) anywhere in the world; this takes the articulation of a subset of criminal policy out of the hands of individual nations and thereby eliminates the possibility of inconsistencies.[249] The viability of the system is in doubt, however, due to countries' disinclination to surrender domestic law in favor of global cybercrime laws.

The alternative is to create a template, a set of principles countries can utilize in adopting cybercrime-specific law and/or in amending their existing laws to ensure that they adequately encompass the use of computer technology to commit traditional offenses.[250] This is, as Section III(A)(3) explains, the approach the Council of Europe has taken in its Convention on Cyber-Crime. The first section below examines this alternative, analyzing the principles that might be used to create such a template or, in the more commonly used phrase, a set of "consensus crimes."[251] The second section discusses the extent to which countries have already achieved some consensus in this regard, while the third section considers the likelihood of achieving further consensus on these issues.

1. CONSENSUS CRIMES: WHAT ARE THEY?

The notion of consensus crimes is oxymoronic insofar as it implies there are fundamental differences in the way nations go about defining the conduct that will result in the imposition of a society's harshest sanctions.[252] In fact, there is a great deal of consistency, across geography and across time, in how countries delineate outlawed behaviors.[253]

March 24, 1995, *available at* http://net.unl.edu/~swi/pers/nazi.html (Gary Lauck, an American citizen who distributed pro-Nazi materials, was arrested by police in Europe and extradited to Germany, where he was convicted of inciting racial hatred and disseminating illegal propaganda).

[249] *See, e.g., Conclusions of the Study on Effective Measures to Prevent and Control High-Technology and Computer-Related Crime*, *supra* note 30, at item 4 at 15 (possibility of creating a legally binding international instrument addressing cybercrime).

[250] *See* § II(A), *supra* (cybercrimes consists of using computer technology to commit new types of crime and to commit traditional crimes in new ways).

[251] *See* § III(B)(1), *infra*.

[252] *See, e.g.,* S. SHAVELL, PRINCIPLES OF ECONOMIC ANALYSIS OF LAW Ch. 24 p. 2 (2000), *available at* http://econ.bu.edu/Weiss/Ec337/Shavell/bg24-2e.pdf ("Imprisonment is a sanction that is unique to criminal law, as are . . . whipping, amputation of limbs, . . . banishment and the death penalty").

[253] *Compare* Indian Penal Code (1860), http://www.indialawinfo.com/bareacts/ipc.html, *with* American Law Institute, Model Penal Code (1962).

This consistency derives from the function of criminal law: to maintain social order within a society.[254] To do that, countries must establish prohibitions that are designed to maintain the integrity of certain vital interests: the safety of persons; the security of property; the stability of the government; and the sanctity of particular moral principles.[255] No society can survive if its constituents are free to harm each other at will, to appropriate each other's property, to undermine the political order and/or to flout the moral principles the citizenry hold dear. Every society will therefore formulate penal prohibitions defining (i) crimes against persons (e.g., murder, assault, rape); (ii) crimes against property (e.g., theft, arson, fraud); (iii) crimes against the state (e.g., treason, rioting, obstruction of justice); and (iv) crimes against morality (e.g., obscene materials, defiling a place of worship).[256]

The greatest degree of consistency will be found in the first two categories which represent the *malum in se* crimes, the absolute prohibitions a society must establish if it is to maintain a modicum of social order because they involve the direct infliction of harm by one person upon another or others.[257]

---

[254] *See, e.g.,* The Code of Hammurabi, http://www.yale.edu/lawweb/avalon/hamframe.htm. *See also* ROLLIN M. PERKINS & RONALD N. BOYCE, CRIMINAL LAW 5 (3d ed. 1982) ("The purpose of the criminal law is to define socially intolerable conduct, and to hold conduct within the limits which are reasonably acceptable from the social point of view").

[255] *See, e.g.,* Portugal, Código Penal, http://www.cea.ucp.pt/lei/penal/penalind.htm; Criminal Code of the Russian Soviet Federated Socialist Republic (1934), http://www.tiac.net/users/hcunn/rus/uk-rsfsr.html. *See generally* 4 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND *5-*7. *See also* ANDREW ASHWORTH, PRINCIPLES OF CRIMINAL LAW 11 (1991).

[256] *See, e.g.,* H.L.A. Hart, *Law as the Union of Primary and Secondary Rules,* THE NATURE OF LAW 144, 145 (M. P. Golding ed. 1966) (a society must enact "in some form restrictions on the free use of violence, theft, and deception to which human beings are tempted but which they must, in general, repress if they are to coexist in close proximity to each other"). *See also* Criminal Code of the Republic of Belarus, http://www.belarus.net/softinfo/lowcatal.htm; Bulgaria Penal Code, http://www.umt.edu/lawinsider/library/lawbyjur/bulgarpc.htm; Criminal Law of the People's Republic of China, http://www.qis.net/chinalaw/prclaw60.htm; Estonian Penal Code, http://www.legaltext.ee/en/andmebaas/ava.asp?m=026; Fiji Islands Penal Code, http://www.vanuatu.usp.ac.fj/paclawmat/Fiji_legislation/Consolidation_1978/Fiji_Penal_Code.html; German Penal Code, http://www.bmj.bund.de/publik/e_stgb.pdf; The Indian Penal Code, http://www.fordham.edu/halsall/india/manu-full.html; Malaysia Penal Code, http://www.lawnet.com.my/lawnet/penalcode.html; Revised Penal Code of the Philippines, http://www.chanrobles.com/revisedpenalcodeofthephilippinesbook2.htm; Criminal Code of the Russian Soviet Federated Socialist Republic (1934), http://www.tiac.net/users/hcunn/rus/uk-rsfsr.html; Sweden, Penal Code (1999), http://justitie.regeringen.se/propositionermm/ds/pdf/Penalcode.pdf; Penal Code of the United Arab Emirates (1988); Zamfara State of Nigeria, Shari'ah Penal Code Law (Jan. 2000), http://www.nigerianlaws.com/frames/docs/stats/ShariaCodeContents.html. *See also* American Law Institute, Model Penal Code (1962); Paul H. Robinson, A Draft Code of Conduct, http://wings.buffalo.edu/law/bclc/rbnsncon.htmhttp://wings.buffalo.edu/law/bclc/rbnsncon.htm. *See generally* Anglo-Saxon Law – Extracts from the Early Laws of the English, http://www.yale.edu/lawweb/avalon/medieval/saxlaw.htm; The Code of Hammurabi, http://www.yale.edu/lawweb/avalon/hamframe.htm; The Salic Law, http://www.yale.edu/lawweb/avalon/medieval/salic.htm; The Visigothic Code, http://libro.uca.edu/vcode/.

[257] "A crime which is malum in se is . . . 'naturally evil, such as murder, rape, arson, burglary, and larceny'. . . . A crime which is malum prohibitum is one prohibited by statute . . . 'although no moral turpitude or dereliction may attach.'" State v. Hertzog, 615 P.2d 480, 489 (Wash. Ct. App. 1980) aff'd in part, rev'd in part, 635 P.2d 694 (Wash. 1981). Since notions of what is "evil" can vary between societies, a more useful distinction is that

There will be consistency as to a core of offenses in the third category, e.g., treason, riot, and obstructing justice, because every society must also ensure the stability of its political order.[258] But there will be more overall deviation in this category because nations vary in terms of the extent to which they feel it necessary to discourage political dissidence.[259] Finally, there will be a great deal of inconsistency as to offenses in the fourth category because they are the product of a society's values and religious principles and, as such, tend to be much more idiosyncratic in nature.[260]

How is this relevant to the development of consensus related to high-tech crimes? For one thing, any effort to devise consensus crimes as an instrument for harmonizing national cybercrime laws needs to take account of, and build upon, consistencies that exist in the articulation of terrestrial crimes. The more these consensus crimes mirror the definitions of traditional crimes, the more likely it is that countries will be willing to incorporate them into their penal codes. It will, for example, be easier to devise consensus crimes that deal with *malum in se* offenses such as burglary, larceny and property damage than with crimes such as pornography or gambling because the definitions of the former will be far more consistent across national boundaries than the latter. All countries will outlaw acts falling into the first category, and will do so in relatively standard terms because the prohibitions are directed at a finite range of conduct.[261]

> malum in se crimes can be defined as involving acts or threats of force, theft, or fraud--i.e., offenses against particular persons or their property. Malum prohibitum crimes can then be defined as those offenses that lack the element of direct injury or harm to specific individuals but are prohibited because their negative consequences are borne by society at large. For example, armed robbery involves the taking of another person's property by means of violence or threats of violence and therefore would be classified as malum in se. Simple drug possession, in contrast, lacks any direct element of force, theft, or fraud but is made criminal because . . . those who possess drugs are likely to commit acts of force, theft or fraud. . . .

Erik Luna, *Principled Enforcement of Penal Codes*, 4 BUFF. CRIM. L. REV. 515, 526 n. 42 (2000), *available at* http://wings.buffalo.edu/law/bclc/bclrarticles/4(1)/lunapdf.pdf.

[258] *See, e.g.,* Fiji Islands Penal Code, §§ 50 (treason), 87 (unlawful assembly) & 130 (destroying evidence), *available at* http://www.vanuatu.usp.ac.fj/paclawmat/Fiji_legislation/Consolidation_1978/Fiji_Penal_Code.html; Revised Penal Code of the Philippines, Articles 114 (treason), 153 (tumults and other disturbances of public order) & 180-181 (false testimony), *available at* http://www.chanrobles.com/revisedpenalcodeofthephilippinesbook2.htm.

[259] *See, e.g.,* Criminal Code of the Russian Soviet Federated Socialist Republic (1934), § 58-12, *available at* http://www.tiac.net/users/hcunn/rus/uk-rsfsr.html ("Failure to denounce a counterrevolutionary crime, reliably known to be in preparation or carried out, shall be punishable by . . . deprivation of liberty for a term not less than six months").

[260] *Compare* Zamfara State of Nigeria, Shari'ah Penal Code Law (Jan. 2000), §§ 126 & 127 (fornication and adultery offenses), *available at* http://www.nigerianlaws.com/frames/docs/stats/ShariaCodeContents.html with CONN. GEN. STAT. § 53a-81 (adultery offense repealed) *and* D.C. CODE ANN. § 22-1001 (fornication offense repealed). *See also* Fiji Islands Penal Code, §§ 145 (insult to religion) & 232 (witchcraft and sorcery), *available at* http://www.vanuatu.usp.ac.fj/paclawmat/Fiji_legislation/Consolidation_1978/Fiji_Penal_Code.html; Revised Penal Code of the Philippines, Article 200 (grave scandal), *available at* http://www.chanrobles.com/revisedpenalcodeofthephilippinesbook2.htm; United Arab Emirates Penal Code Article 358 (1988) (offense of committing "publicly an infamous act constituting a violation of the rules of decency").

[261] *Compare* Criminal Law of the People's Republic of China, Article 263 (robbery), *available at* http://www.qis.net/chinalaw/prclaw60.htm#Chapter%20V2 *with* German Penal Code §§ 249 & 250 (robbery), *available at* http://www.bmj.bund.de/publik/e_stgb.pdf *and* United Arab Emirates Penal Code Articles 383 & 384 (1988) (robbery).

As to pornography and gambling, countries will vary widely in their prohibitions of the former,[262] and some will, and some will not, prohibit the latter.[263] Building upon previously existing legal concepts also makes the process more efficient and more effective; trying to create new law from scratch is a very time-consuming process, and the technology and the threat is constantly marching on.

For another, identifying fundamental consistencies in the structure of penal codes can help to identify those areas where consensus crimes are most likely to be needed. Unlike civil statutes, which tend to prescribe standards and behaviors,[264] criminal statutes are prohibitionary, i.e., they prohibit the behaviors used to achieve specified results.[265] A criminal statute is designed to prevent a forbidden result, or "harm," by outlawing it and imposing a more or less heinous penalty upon those who achieve (and who endeavor to achieve) that result.[266] The focus of such a statute is therefore on the prohibited result, and its ability to encompass the use of computer technology in achieving that result will depend on the extent to which the statute is phrased in terms that transcend the differences between physical reality and virtual reality.[267]

a. CRIMES AGAINST PERSONS

It is, for example, almost certain there will be no need to devise consensus crimes addressing homicide and rape, albeit for different reasons. The purpose of developing consensus crimes is to provide a means of filling the gaps in a country's existing penal law that do not allow the prosecution of cybercrimes.[268] Gaps exist either (a) because a country has not yet outlawed entirely "new" types of criminal activity (such as cyberstalking)[269] or (b) because the language a country has employed to define traditional crimes is so based in physical reality it cannot encompass the use of computer technology to commit those crimes.[270] Since both homicide and rape, perhaps the oldest forms of criminal activity, are

---

[262] *Compare* KAN. STAT. ANN. § 21-4302 (promoting obscenity) *with* Sweden, Penal Code (1999), *available at* http://justitie.regeringen.se/propositionermm/ds/pdf/Penalcode.pdf (no obscenity offense).

[263] *See, e.g.,* William R. Edington, *Casinos and Tourism in the 21st Century*, http://www.unr.edu/business/econ/trends2000.html (surveying legalization of gambling).

[264] *See, e.g.,* German Civil Code, Part II – Seventh Section, *available at* http://www.hull.ac.uk/php/lastcb/bgbeng2.htm; The Civil Code of Mongolia, Articles 160-178, *available at* http://www.indiana.edu/~mongsoc/mong/civilcode.htm. Civil statutes that sound in tort, especially those which deal with intentional torts, tend to be more prohibitionary than prescriptive because they deal with conduct which is analogous to that at issue in criminal statutes.

[265] *See, e.g.,* New South Wales Consolidated Acts: Crimes Act 1900, Part 3 ("offences against the person"), http://www.austlii.edu.au/au/legis/nsw/consol_act/ca190082/; Sweden, Penal Code, Part Two ("on crimes"), http://justitie.regeringen.se/propositionermm/ds/pdf/Penalcode.pdf.

[266] *See, e.g.,* Brenner, *supra* note 91.

[267] *See, e.g., id.*

[268] *See, e.g., Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information*, *supra* note 1.

[269] *See, e.g.,* Brenner, *supra* note 91.

[270] *See, e.g.,* Jari Raman, *Computer Crime*, ENLIST, Nov. 7, 2000, *at* http://itlaw.law.strath.ac.uk/ENLIST/subjects/is/commentary/ ("Some countries are reluctant to apply the traditional

crimes that are firmly grounded in physical reality, neither falls into the first category; every country will have long ago outlawed the acts of taking another person's life and of forcibly having sexual intercourse.[271] Homicide does not fall into the second category because homicide crimes are defined in terms of a prohibited result—the death of another person or persons--that transcends the differences between physical and virtual reality.[272] The focus is on the result--the method is for the most part irrelevant.[273] Penal codes do not, for instance, parse the result into "homicide by gun," "homicide by strangulation," "homicide by poison" and so on; they simply prohibit causing the death of another human being.[274] Existing homicides statutes should therefore encompass the use of computer technology to cause the death of another person or persons.[275]

Rape will not fall into the second category as long as it continues to prohibit coerced physical sexual intercourse between two or more people because such an act cannot be consummated in cyberspace or via the medium of computer technology;[276] existing rape statutes should therefore apply even if computer technology were somehow to be used as the means of perpetrating rape (to identify a victim, say).[277] As to other physical crimes against persons, assault-type statutes and kidnapping statutes should be able to encompass whatever role computer technology comes to play in the commission of these crimes;[278] as should child abuse and suicide statutes.[279] The same should generally be true for

---

provision of theft and embezzlement to . . . gathering secret data because these provisions require the taking of tangible property with the intention of permanently depriving the victim of it").

[271] *See, e.g.,* Criminal Law of the People's Republic of China, Articles 232 (homicide) & 236 (rape), *available at* http://www.qis.net/chinalaw/prclaw60.htm#Chapter%20IV2; Fiji Islands Penal Code, §§ 149 (rape) & 199 (murder); Indian Penal Code, §§ 300 (homicide) & 375 (rape), *available at* http://www.indialawinfo.com/bareacts/ipc.html#_Toc496765173; Sweden, Penal Code, Chapter 3 § 1 (homicide) & Chapter 6 § 1 (rape), *available at* http://justitie.regeringen.se/propositionermm/ds/pdf/Penalcode.pdf; United Arab Emirates Penal Code, Articles 332 (homicide) & 354 (rape). *See also* The Code of Hammurabi, *available at* http://www.yale.edu/lawweb/avalon/hamframe.htm; The Visigothic Code, http://libro.uca.edu/vcode/.

[272] *See, e.g.,* Brenner, *supra* note 91.

[273] Some statutes do, of course, provide for the imposition of enhanced penalties if particular weapons (notably firearms) are used to commit a crime against persons. For more on this, and more on its applicability to cybercrime, *see* Brenner, *supra* note 91.

[274] *See, e.g.,* Criminal Law of the People's Republic of China, Art. 232 (homicide), *available at* http://www.qis.net/chinalaw/prclaw60.htm#Chapter%20IV2; Indian Penal Code, § 300, *available at* http://www.indialawinfo.com/bareacts/ipc.html#_Toc496765173; Sweden, Penal Code, Chapter 3 § 1 (homicide), *available at* http://justitie.regeringen.se/propositionermm/ds/pdf/Penalcode.pdf; United Arab Emirates Penal Code, Article 332. *See also* Brenner, *supra* note 91.

[275] *See, e.g.,* Indian Penal Code, § 300 (murder), *available at* http://www.indialawinfo.com/bareacts/ipc.html#_Toc496765173. The Indian Penal Code was originally promulgated on October 6, 1860; its definition of murder is quite adequate to encompass the use of computer technology to take someone's life.

[276] *See, e.g.,* Julian Dibbell, *A Rape in Cyberspace*, at http://www.levity.com/julian/bungle.html. *See also,* Brenner, *supra* note 91.

[277] *See, e.g.,* Sandro Cohen, *Oliver Jovanovic: First Sacrifice of the Digital Age*, May 19, 1998, *at* http://www.ishipress.com/sandro.htm (man accused of raping woman he met over the Internet).

[278] *See, e.g.,* Criminal Law of the People's Republic of China, *available at* http://www.qis.net/chinalaw/prclaw60.htm#Chapter%20IV2 Article 239 (kidnapping); Sweden, Penal Code,

statutes defining non-physical crimes against persons, such as invasions of privacy and defamation.[280] So far, the truly problematic crimes in this category are those targeting harassment or intimidation: The prohibited result is usually a direct threat to cause physical harm to the victim or the victim's family; statutes that prohibit the generic communication of such a threat should reach the use of computer technology to that end.[281] Unfortunately, the Internet and its facilitation of anonymous communication have generated varieties of harassment that do not involve the transmission of a direct threat to cause physical injury and so cannot be prosecuted under existing law; to reach this type of conduct, nations will have to enact statutes that broaden the prohibited result.

b. CRIMES AGAINST PROPERTY

What about crimes against property? The prohibited results are wrongfully taking another's property (embezzlement, theft, robbery, fraud, forgery); wrongfully damaging or destroying another's property (vandalism, arson); and wrongfully intruding upon another's property (trespass, burglary).[282]

Chapter 3 § 5 (assault) & Chapter 4 § 1 (kidnapping), *available at* http://justitie.regeringen.se/propositionermm/ds/pdf/Penalcode.pdf; Zamfara State of Nigeria, Shari'ah Penal Code Law (Jan. 2000), § 223 (assault) & § 229 (kidnapping), *available at* http://www.nigerianlaws.com/frames/docs/stats/ShariaCodeContents.html.

[279] *See, e.g.,* Sweden, Penal Code, Chapter 6 § 7 (child molestation), *available at* http://justitie.regeringen.se/propositionermm/ds/pdf/Penalcode.pdf; Zamfara State of Nigeria, Shari'ah Penal Code Law (Jan. 2000), § 213 (cruelty to children), *available at* http://www.nigerianlaws.com/frames/docs/stats/ShariaCodeContents.html; Fiji Islands Penal Code §§ 155 (child molestation) & 219 (liability for another's suicide), *available at* http://www.vanuatu.usp.ac.fj/paclawmat/Fiji_legislation/Consolidation_1978/Fiji_Penal_Code.html. *See also* Indian Penal Code §§ 306 & 309 (aiding suicide & attempting suicide), *available at* http://www.indialawinfo.com/bareacts/ipc.html.

[280] *See, e.g.,* Indian Penal Code, § 499, *available at* http://www.indialawinfo.com/bareacts/ipc.html#_Toc496765395:

> Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person.

This provision—from a penal code that was drafted in 1860—is broad enough to encompass the use of the Internet to distribute defamatory comments.

[281] *Cf.* New South Wales Consolidated Acts, Crimes Act 1900, § 31 ("documents containing threats"), *available at* http://www.austlii.edu.au/au/legis/nsw/consol_act/ca190082/s31.html.

[282] *See, e.g.,* Criminal Code of the Republic of Belarus, Chapter 7 ("Crimes Against Property"), http://www.belarus.net/softinfo/catal_la/l00097.htm; Canada, Criminal Code, Part IX ("Offenses Against Rights of Property"), http://laws.justice.gc.ca/en/C-46/index.html (last modified Aug. 31, 2001); Criminal Law of the People's Republic of China, Article 263, http://www.qis.net/chinalaw/prclaw60.htm (Mar. 14, 1997); Fiji Islands Penal Code, §§ 258-351, http://www.vanuatu.usp.ac.fj/paclawmat/Fiji_legislation/Consolidation_1978/Fiji_Penal_Code.html; INDIA PEN. CODE, §§ 378-480, http://www.indialawinfo.com/bareacts/ipc.html#_Toc496765051; Zamfara State of Nigeria, Shari'ah Penal Code Law (Jan. 2000), §§ 144, 161, 173, & 179 http://www.nigerianlaws.com/frames/docs/stats/ShariaCodeContents.html (Jan. 27, 2000).

Since crimes against property are also among the oldest types of criminal activity, prohibitions directed at these results are standard features of every penal code.[283]

Computer technology makes the application of these prohibitions problematic in certain respects. Unlike the harassment statutes discussed in the preceding paragraph, the problem here lies not with the characterization of the prohibited results but with the conceptualization of "property." The formulations of offenses falling into this category have always been predicated upon the notion that "property" is a real-world, physical construct, i.e., a tangible item.[284] Conceptualizing property in this way imposes significant limitations upon the application of theft, damage and intrusion statutes to conduct occurring in and via cyberspace because in cyberspace property becomes an intangible item. Cyberspace property can consist, for instance, of electronic data which has value because it represents funds one can expend in the "real world"; cyberspace property also consists of software, of domain names and of "pure" information, all of which are valuable in and of themselves. Some transgressions against intangible property can be prosecuted using traditional crimes against property statutes, but some cannot. If a hacker breaks into a bank's computer system and electronically transfers $1 million from Bill Gates' account into an account she controls, this is theft, even under traditional theft statutes; the possession and use of the funds has been completely transferred from Gates to the hacker even though at no time did the hacker have physical possession of real currency.

But if a hacker breaks into the computer system of a biotech research corporation, copies secret information about the company's research and takes the copies, this is not theft in the traditional sense because the company has not been totally deprived of the information; it still has its property, though the value of that property has no doubt been diluted by the thief's actions.[285] The same tends to be true of property damage or destruction statutes, which were drafted to prohibit the acts of damaging or destroying tangible property;[286] it may, for example, be impossible to use a vandalism statute to prosecute a hacker who defaces a web site.[287] Property intrusion statutes also suffer from the same defect in characterization, though it plays a somewhat different role in this context. Criminal trespass and burglary statutes were developed to deal with persons who physically entered a material space—real world property--without being authorized to do so.[288] Since these statutes require an actual physical intrusion into a tangible physical area, they cannot be used to prosecute a hacker who metaphorically "breaks into" a computer system; while the computer system is itself a form of real world property, and while the hacker does in a sense "enter into" that system, the concepts traditionally used to operationalize the trespass crimes simply do not apply to the hacker's conduct. Consensus crimes are, therefore, needed to update the traditional categories of crimes against property.

---

[283] *See id.*

[284] *See, e.g.,* INDIA PEN. CODE, § 22 ("corporeal property of every description, except land and things attached to the earth"), http://www.indialawinfo.com/bareacts/ipc.html#_Toc496765051.

[285] Under some circumstances, this would be covered by industrial/economic espionage statutes.

[286] *See, e.g.,* INDIA PEN. CODE, § 425, http://www.indialawinfo.com/bareacts/ipc.html#_Toc496765051.

[287] *See, e.g.,* CAL. PENAL CODE § 594 (defining vandalism as causing injury or damage to "any real or personal property"); OHIO REV. CODE § 2909.05 (defining vandalism as causing "serious physical harm" to property). *See also* CAL. PENAL CODE § 7(11) (defining real property) & § 7(12) (defining personal property as including "money, goods, chattels, things in action and evidences of debt").

[288] *See, e.g.,* INDIA PEN. CODE, §§ 441-453, http://www.indialawinfo.com/bareacts/ipc.html#_Toc496765051.

Computer technology has also produced an activity which has all the hallmarks of a crime against property but which does not fit into any of the existing offense categories. Section II(B) described denial of service attacks, in which the attacker shuts down a web site. When a commercial web site is attacked, the site becomes inaccessible to visitors and the operator of the site loses some volume of business. The victim has clearly been deprived of "property," in the form of the lost revenues, but this is not theft because the attacker has not been enriched; the attacker has not appropriated any property from the victim.[289] It is not vandalism because the web site has not been physically damaged or destroyed; and it is not trespass because the attacker never penetrates the victim's web site—the attack is mounted from the outside. It is, however, a crime against property; just as in traditional crimes against property, the victim sustains a loss as the result of the criminal's acts.[290] This, then, is an area in which a consensus crime must be devised to deal with a "new" type of cybercrime.

c. CRIMES AGAINST THE STATE

The third category - crimes against the state - consists of a set of core offenses every country will outlaw plus another set of distinctive offenses found in one or more nations. The core offenses include the crimes of treason, counterfeiting, rioting, and obstructing justice.[291] Treason, the act of levying war against one's country or supporting its enemies, is a crime the prohibitions of which, like those directed at homicide, are very much focused on a specific result;[292] traditional treason statutes should therefore encompass the use of computer technology to achieve this result, so that neither new, cyber-treason statutes nor modifications in existing statues will be required.[293] Traditional rioting statutes may not encompass the use of computer technology to instigate rioting or other forms of public disorder,[294] so this is an area where new legislation can be needed. Computer technology should not affect the application of traditional counterfeiting statues since, as one author noted, "[u]sing a computer, a scanner, graphics software, and a high-quality color laser printer for forgery or counterfeiting is the same crime as using an

---

[289] *See, e.g.,* Charlie Baggett, *Denial of Service: The New Cyber Terror,* BIZMONTHLY.COM, March, 2000, http:/www.bizmonthly.com/3_2000/baggett.html.

[290] One could analogize it to extortion under the Hobbs Act, 18 U.S. Code § 1951(a). Federal courts have held that since the right to conduct a lawful business is "property" within the meaning of the Hobbs Act, abortion protestors can be prosecuted for "extortion" when they interfere with an abortion clinic's right to conduct business even though the protestors' actions are not designed to appropriate property belonging to the clinics. *See, e.g.,* United States v. Arena, 918 F. Supp. 561, 568-569 (N.D.N.Y. 1996).

[291] *See, e.g.,* Criminal Law of the People's Republic of China, Articles 102-113, 170, http://www.qis.net/chinalaw/prclaw60.htm (Mar. 14, 1997); Fiji Islands Penal Code, §§ 50-68, 79-105, 117-136, 352-368, http://www.vanuatu.usp.ac.fj/paclawmat/Fiji_legislation/Consolidation_1978/Fiji_Penal_Code.html.

[292] *See, e.g.,* Fiji Islands Penal Code, § 50, http://www.vanuatu.usp.ac.fj/paclawmat/Fiji_legislation/Consolidation_1978/Fiji_Penal_Code.html.

[293] *Cf.* 18 U.S.C.S. Code § 1030(a)(1) (2001) (stating that it is a crime to access computer containing information vital to the security of the United States of America without authorization, copy that information and give it to a foreign nation believing it could be used to injury the U.S.).

[294] *See, e.g.,* Fiji Islands Penal Code, § 86, http://www.vanuatu.usp.ac.fj/paclawmat/Fiji_legislation/Consolidation_1978/Fiji_Penal_Code.html; INDIA PEN. CODE, § 146, http://www.indialawinfo.com/bareacts/ipc.html#_Toc496765051. *But see* INDIA PEN. CODE, § 150, http://www.indialawinfo.com/bareacts/ipc.html#_Toc496765051 ("Whoever . . . promotes . . . any person to join or become a member of any unlawful assembly" is guilty of unlawful assembly, or rioting).

old-fashioned printing press with ink".[295] Obstructing justice is an area where existing laws may need to be modified: Statutes in this area prohibit, among other things, creating, modifying or destroying evidence; to the extent that such statutes conceptualize evidence solely as a tangible commodity,[296] they will need to be modified to include acts directed at electronic evidence. Also, existing obstruction of justice statutes may not address acts such as, for example, hacking into a court system's computers and altering or deleting charges against a perpetrator or warrants issued for his arrest.[297]

While it might seem that these issues are a matter of local concern, and therefore not the likely focus of consensus crime categories, that is in fact not the case; the transnational character of cybercrime means that countries depend upon each other, in large part, to gather and preserve evidence and, to a lesser extent, to facilitate the identification and apprehension of known offenders. If a cybercriminal can exploit loopholes in one country's obstruction of justice laws, this can have a negative impact on other countries, the citizens of which have been victimized by that cybercriminal's activities.

d. CRIMES AGAINST MORALITY

The fourth and final category - crimes against morality - is the one in which there will be the least consistency in the creation and definition of offenses.[298] This lack of consistency has two implications for the articulation of consensus crimes: the lack of consistency means that what is a crime in some countries (gambling, say) is not a crime elsewhere, so this category is *generally* not likely to be a source of consensus crimes; the lack of consistency also means that it would *generally* be difficult to gain acceptance for consensus crimes developed for this category. The qualifications are necessary because it is sometimes difficult to decide whether an activity—such as child pornography—is a "crime against persons" or a "crime against morality." Child pornography, at least non-virtual child pornography, clearly falls into both categories: a crime against persons is committed when real children are used to

---

[295] Ronald B. Standler, *Computer Crime* (1999), http://www.rbs2.com/ccrime.htm. *But see* INDIA PEN. CODE § 231, http://www.indialawinfo.com/bareacts/ipc.html#_Toc496765051 (making it an offense to counterfeit "coin"). Conventional counterfeiting statutes might have to be amended to encompass electronic currency. *See generally* Jean Camp, et al., *Token and Notational Money in Electronic Commerce*, http://citeseer.nj.nec.com/camp95token.html*; U.S. Department of the Treasury, An Introduction to Electronic Money Issues 26 (1996),* http://www.occ.treas.gov/netbank/paper.pdf.

[296] *See, e.g.,* INDIA PEN. CODE § 192, http://www.indialawinfo.com/bareacts/ipc.html#_Toc496765051. *See generally* Criminal Law of the People's Republic of China, Article 306, http://www.qis.net/chinalaw/prclaw60.htm (Mar. 14, 1997); New South Wales Consolidated Acts, Crimes Act 1900, § 317, http://www.austlii.edu.au/au/legis/nsw/consol_act/ca190082/s317.html.

[297] *See, e.g.,* Jonathan Saltzman, *Traffic Clerk Charged with Erasing Fines,* PROVIDENCE J, March 7, 2000, A1, *available at* 2000 WL 5096652; *Campaign Donor Is Indicted,* WASH. POST, Jan. 9, 2000, at A15, http://www.washingtonpost.com/wp-srv/WPlate/2000-01/09/172l-010900-idx.html; Rowan Scarborough, *Army Files 17 Charges against General Hale,* WASHINGTON TIMES, Dec. 12, 1998, http://reagan.com/HotTopics.main/HotMike/document-12.11.1998.3.html; *Student Accused of Erasing Traffic Tickets from Court Computer,* DETROIT NEWS, April 26, 1997.

[298] *Compare* Fiji Islands Penal Code §§ 145-186, http://www.vanuatu.usp.ac.fj/paclawmat/Fiji_legislation/Consolidation_1978/Fiji_Penal_Code.html *with* Criminal Law of the People's Republic of China, Articles 249-252, 258-261, http://www.qis.net/chinalaw/prclaw60.htm#Chapter%20IV2 (Mar. 14, 1997) *and* Estonian Penal Code, §§ 154-155 176-182, 202, http://www.legaltext.ee/en/andmebaas/ava.asp?m=026.

produce child pornography;[299] and the creation, distribution and possession of child pornography is considered a crime against morality in many nations,[300] just as the dissemination of adult pornography is often considered to be a crime against morality.[301] Child pornography in some guise is therefore an area that will almost certainly be the focus of one or more consensus crimes. Victimless crimes like the use of drugs and alcohol, gambling and prostitution fall into the category of crimes against morality,[302] but this type of prohibition tends to be so tied into parochial standards of morality it is unlikely to yield consensus crimes. The same is true of offenses that prohibit acts directed at religious observances or symbols.

There are other activities that, like child pornography, do not fit neatly into any one category. Terrorism is one: it can be considered a crime against persons because terrorist acts inflict injury and death, a crime against property because property is often damaged by terrorist acts, and/or a crime against the state because the terrorist's goal is to undermine the stability of that state by generating chaos and destruction.[303] The characterization of terrorism is further complicated by the fact that nations disagree as to what is, and is not, a terrorist act;[304] the British described the American revolutionaries as terrorists but

---

[299]This is not true when child pornography is "virtual." *See, e.g.,* Free Speech Coalition v. Reno, 198 F.3d 1083, 1086-1093, (9th Cir. 1999), *rehearing and suggestion for rehearing en banc denied*, 220 F.3d 1113 (9th Cir. 2000), *cert. granted sub nom.* Ashcroft v. Free Speech Coalition, 531U.S. 1124 (2001).

[300] *Cf.* Sweden, Penal Code (child pornography not criminalized), http://justitie.regeringen.se/propositionermm/ds/pdf/Penalcode.pdf. For a compilation of laws dealing with child pornography, *see* Legislation of Interpol Member States on Sexual Offences Against Children, INTERPOL, http://www.interpol.int/Public/Children/SexualAbuse/NationalLaws/.

[301] *See, e.g., Białystok Blue,* WARSAW VOICE, August 18, 1996, *at* http://www.warsawvoice.pl/v408/News01.html (spokesperson for Ministry of Justice quoted as stating that "[p]ornography is a crime against morality").

[302] *See, e.g.,* Gerard V. Bradley, *Retribution and the Secondary Aims of Punishment,* 44 AM. J. JURIS. 105, 108 (1999) ("The reason for blanket legal prohibitions . . . of drinking or gambling is concern for the character of the morally weak. A culture stripped of certain temptations helps the weak to be good.").

[303] For a definition of terrorism, *see, e.g.,* Yonah Alexander, Director of Terrorism Studies, George Washington University:

> `The deliberate employment of violence or the threat of . . . violence . . . to attain strategic and political objectives. Theses unlawful acts are intended to create overwhelming fear in a target population larger than the civilian or military victims attacked or threatened.'

(quoted in *Terrorism*, http://pweb.bentley.edu/students/s/seferia_davi/id45.htm).

[304] As one source points out, many countries disagree with the conventional definitions of terrorism

> on the basis of two main missing elements. First, . . . no distinction is made between terrorism and violence perpetuated by liberation movements fighting for the freedom of their peoples and countries. Second, they focus on the acts themselves, thereby completely ignoring the root causes which may lead to such acts. . . .
>
> . . . Third World countries . . . are concerned not just about the acts themselves, but also about issues of self-determination, and how this relates to the pursuit of independence from . . . alien domination. . . . Because. . . industrialized countries . . . are the targets of terrorism . . . their view is, understandably quite different. To them, violence against innocents is terrorism; they are not interested in motives or root causes.

to modern Americans they were heroic freedom fighters. For that reason, perhaps, countries tend to prosecute terrorist acts as crimes against persons and crimes against property,[305] reducing the acts to their constituent results instead of treating them as a distinct category of criminal activity. This suggests terrorism is not a likely candidate for a consensus crime.[306]

Analyzing consistencies in the articulation of traditional crimes suggests that consensus crimes are needed and are likely to be accepted in these areas:

- defining "new" crimes against persons, for example, online stalking and harassment;
- revising extant crimes against property so they encompass acts directed at intangible property;
- defining "new" crimes against property that encompass denial of service attacks and other emerging types of property damage;
- revising obstruction of justice crimes so they encompass, *inter alia,* the creation, alteration, admissibility and destruction of electronic evidence;
- defining "new" crimes directed at obstructing justice, such as tampering with court records; and
- revising some crimes against morality, notably child pornography, to encompass the use of computer technology.

Since the property crimes are the most consistently problematic, and since the business community and global financial markets have an enormous stake in ensuring the safety of property, this area will no doubt be among the first of these to be addressed. The analysis of consistencies in the articulation of traditional crimes also suggests that consensus crimes are otherwise not likely to be developed (a) because cybercrime can be prosecuted under existing offense-definitions or (b) because there is a lack of agreement between nations as to what should and should not be criminalized. And while it may seem as if consensus might be an impossible goal to reach, evidence would suggest that more and more nations around the world are moving towards consensus in their approaches to crime in cyberspace.

2. EFFORTS TO BUILD CONSENSUS

Though some might look at the recently adopted Council of Europe Treaty on Cybercrime and suggest that the notion of building consensus on crime in cyberspace is a relatively new phenomenon, a review of history clearly shows consensus has been building over the last two decades. Indeed, the need for building consensus is apparent to those involved in combating cybercrime. Thus, there have been a series of efforts undertaken to build consensus around a set of core crimes. The first two sections below examine these efforts;[307] the third section explores impediments to these efforts.[308]

Terrorism, http://pweb.bentley.edu/students/s/seferia_davi/id45.htm .

[305] *See, e.g.,* Criminal Law of the People's Republic of China, Articles 114-124, *at* http://www.qis.net/chinalaw/prclaw60.htm (Mar. 14, 1997). *See also* United States v. Bin Laden, et al., Indictment S(9) 98 Cr. 1023 (LBS), Southern District of New York, http://www.fbi.gov/majcases/eastafrica/indictment.pdf (indictment in Kenya and Tanzania embassy bombings charged defendants with 229 counts of murder plus conspiracy, perjury, attempted murder, attempt to take hostage and assaults).

[306] *But see* § III(B)(1)(b), *infra*.

[307] *See* §§ III(B)(2)(a)-(b), *infra.*

a. REVIEW OF EFFORTS TO BUILD CONSENSUS

Section III(A)(3) describes international efforts to build consensus around a set of core cybercrimes in some detail. It is useful to review those efforts here, to set the stage for a discussion of where consensus currently exists and where it is, and is not, likely to be developed.

In 1986, the Organization for Economic Cooperation and Development issued a report that contained a list of acts countries should criminalize; aside from software piracy, the acts involved attacks on computers, computer systems or computer data.[309] In 1989, the Council of Europe's Select Committee of Experts on Computer-Related Crime issued a similar list,[310] which became the foundation of the Convention on Cyber Crime that is discussed below.[311]

In 1990, the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders produced a resolution that called for Member States to modernize their laws by, among other things, creating offenses, where necessary, to "deal with this novel and sophisticated form of criminal activity".[312] While the United Nations' work in 1990 produced a number of resolutions related to cybercrime, information security, and the protection of privacy, it wasn't until 1994 that the UN published its *Manual on the Prevention and Control of Computer-related Crime*, wherein specific computer related crimes were introduced and explained to member nations.[313] The UN *Computer Crime Manual* was not put forth as a treaty remedy per se, rather it was educational in nature. The manual however did recognize the need for consensus vis-à-vis cybercrime:

> Given the international scope of telecommunications and computer communications, the transborder nature of many computer crimes and the acknowledged barriers within current forms of international cooperation, a concerted international effort is required to address the problem effectively. Attempts to define computer crime, or at least achieve common conceptions of what is comprises, and to harmonize the procedural processes for sanctioning it have a number of benefits.…[314]

As the above paragraph suggests, the benefits of building consensus around offenses to be prohibited in cyberspace has been building for sometime. As time passed, the call for consensus became not only louder and more clear, but also more specific and well honed. That is to say, supra national

---

[308] *See* § III(B)(2)(c), *infra.*

[309] *See* § III(A)(3), *supra.*

[310] *See* § III(A)(3), *supra.*

[311] *See* § III(B)(2)(a)(i), *infra.*

[312]UNITED NATIONS MANUAL ON THE PREVENTION AND CONTROL OF COMPUTER-RELATED CRIME, *supra* note 165, at Introduction – paragraph 18. *See* § III(A)(3), *supra.*

[313] *See* § III(A)(3), *supra.*

[314]UNITED NATIONS MANUAL ON THE PREVENTION AND CONTROL OF COMPUTER-RELATED CRIME, *supra* note 165, at § II(C)(2) - ¶ 117, paragraph 292.

cooperative bodies continued to present with greater and greater detail not only substantive criminal laws to be adopted to combat cybercrime, but a number of procedural legal changes as well.

In 1997, Ministers of the Group of Eight adopted an Action Plan to Combat High-Tech Crime in which the Member States each pledged to review their legal systems to ensure that they "appropriately criminalize abuses of telecommunications and computer systems".[315] Work of the G8 is ongoing and a number of subsequent conferences, meetings, and sub-group get-togethers have taken place.[316]

In 2000, the European Commission issued a report announcing anti-cybercrime measures the Commission planned to take; these measures focused on the adoption of penal law outlawing various activities, which not only included attacks on computer systems but also addressed the use of the Internet to disseminate child pornography and hate speech and its role in promoting the trafficking of illegal drugs.[317] And in November, 2001, the Council of Europe's Convention on Cyber-Crime, which is discussed in the following section, was opened for signature.

b. TWO CURRENT PROPOSALS FOR THE ARTICULATION OF CONSENSUS CRIMES

If the propositions set out in Section III(B)(1) are valid, then consensus crime proposals should target the four areas listed in that section.[318] As the previous section notes, there have been a number of attempts seeking to promote the definition of consensus crimes; for the purposes of this discussion it is sufficient to analyze two such efforts, because they illustrate the types of activities these attempt focus on. One is the Council of Europe's Convention on Cyber Crime that is described in Section II(A)(3); the other is a proposal drafted by the Center for International Security and Cooperation (CISAC).[319] The first two sections below assess the extent to which these Conventions conform to the propositions enunciated above.

i. COUNCIL OF EUROPE CONVENTION

The consensus crime provisions of the Council of Europe's Convention on Cyber Crime conform to the propositions set out above. The Convention does not itself define the crimes as to which it seeks consensus; instead, the Convention lists nine offense categories, and parties to the Convention agree to "adopt such legislative and other measures" as are necessary to define the activity encompassed by each

---

[315] Action Plan to Combat High-Tech Crime, Item #3, Meeting of the Justice and Interior Ministers of The Eight, December 9-10, 1997, COMMUNIQUE ANNEX, WASHINGTON, D.C., http://www.cybercrime.gov/action.htm. *See* § III(A)(3), *supra.*

[316] *See* § III(A)(3), *supra.*

[317] *See* § III(A)(3), *supra.*

[318] *See* § III(B)(1), *supra.*

[319] *See* Center for International Security and Cooperation, A Proposal for an International Convention on Cyber Crime and Terrorism (Aug. 2000), http://www.oas.org/juridico/english/monograph.htm [hereinafter CISAC Convention].

category "as criminal offences under [their] domestic law."[320] The nine categories represent eight property crimes and one non-property crime:[321] illegal access; illegal interception; data interference; system interference; misuse of devices; forgery; fraud; child pornography; and copyright infringement and related offenses.[322]

The first five offense categories are all concerned with outlawing "new" crimes against property; they do this, for the most part, by requiring signatory nations to adopt legislation creating electronic versions of existing property crimes. The illegal access provision requires them to make electronic trespass, or hacking, illegal.[323] The illegal interception provision requires the creation of an electronic invasion of privacy/burglary offense that prohibits unauthorized intrusions resulting in the appropriation of "property" in the form of data.[324] The data interference provision requires the creation of a property damage offense, the "property" again being data.[325] The system interference provision deals with conduct which has no analogue in terrestrial crime, so it requires signatory nations to create a entirely new offense (or offenses) that criminalize denial of service attacks and the dissemination of viruses and other malicious codes.[326] Finally, the misuse of devices provision requires signatory nations to outlaw electronic burglary tools, that is, to make it a crime to produce, sell, procure, import and/or distribute tools to be used in committing any of these four property crimes.[327] This is, first of all, an inchoate offense that targets preparatory steps (e.g., procuring such tools) taken toward committing the target crimes;[328] it also imposes aiding and abetting liability upon those who provide tools that are actually used to commit one of

[320]Council of Europe, Convention on Cybercrime (ETS No. 185), § 1 – Article 2, (November 23, 2001), http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm. *See* § II(A)(3), *supra.*

[321] *See* id., at § 1.

[322] *See id. See also* § II(A)(3), *supra.* It also contains provisions on aiding and abetting and attempt liability, but inchoate and imputed liability are outside the scope of this discussion. The Convention does not define the offenses falling into these categories; parties to the Convention pledge to adopt such "legislative and other measures" as are necessary to outlaw these types of conduct. *See id.*

[323] *See* Explanatory Report, Council of Europe, Convention on Cybercrime, ¶ 44 (November 8, 2001), http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm.

[324] *See* Explanatory Report, Council of Europe, Convention on Cybercrime, ¶¶ 51-58 (November 8, 2001), http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm.

[325] *See* Explanatory Report, Council of Europe, Convention on Cybercrime, ¶ 60 (November 8, 2001), http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm ("The aim of this provision is to provide computer data and computer programs with protection similar to that enjoyed by corporeal objects against intentional infliction of damage").

[326] *See* Explanatory Report, Council of Europe, Convention on Cybercrime, ¶¶ 65-67 (November 8, 2001), http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm.

[327] *See* Explanatory Report, Council of Europe, Convention on Cybercrime, ¶ 71 (November 8, 2001), http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm (directed at outlawing "`hacker tools'"). *See also* ALASKA STAT. § 11.46.315 (possession of burglary tools an offense).

[328] *See, e.g.,* MODEL PENAL CODE § 5.06(1) (possessing instruments of crime); Commonwealth v. Crocker, 389 A.2d 601, 603 (Pa. Super. Ct. 1978). *See also* Ira P. Robbins, *Double Inchoate Crimes,* 26 HARV. J. ON LEGIS. 1, 23-24 (1989).

these crimes;[329] and it imposes an inchoate, attempt-to-aid-and-abet liability upon those who produce and distribute such tools regardless of whether they are actually used to commit one of those crimes.[330]

Three of the next four offense categories also deal with property crimes, but they are not concerned with defining "new" crimes: One requires signatory nations to outlaw computer-related fraud,[331] another does the same for computer-related forgery,[332] and the third requires nations to criminalize computer-related infringements of copyrights and related rights.[333] All three deal with updating traditional property crimes to incorporate the use of computer technology as a tool for committing the crime; infringement of copyright and related rights is, after all, simply a form of theft, i.e., the misappropriation of intangible property.[334]

The non-property crime is child pornography: The Convention requires signatory nations to "modernize" their law so it "more effectively circumscribe[s] the use of computer systems" to produce, distribute and/or possess child pornography.[335] The architects of the Convention recognized that most countries already criminalize these activities, but thought it advisable to emphasize that laws need to be modernized to address "the ever-increasing use of the Internet as the primary instrument for trading such material."[336]

ii. CISAC CONVENTION

---

[329] *See, e.g.,* MODEL PENAL CODE § 2.06 (accomplice liability). *See also* United States v. Falcone, 109 F.2d 579, 581 (2d Cir.), *aff'd without passing on the issue*, 311 U.S. 205 (1940).

[330] *See, e.g.,* MODEL PENAL CODE § 5.01(3) ("A person who engages in conduct designed to aid another to commit a crime . . . is guilty of an attempt to commit the crime, although the crime is not committed or attempted by such other person . . . .").

This provision seems to be redundant because other provisions of the Draft Convention require signatory parties to adopt legislation imposing attempt and aiding and abetting liability as to the offenses defined in accordance with the Convention. *See* Council of Europe, Convention on Cybercrime, *supra* note 320, at § 1, Article 11.

[331] *See* Explanatory Report, Council of Europe, Convention on Cybercrime, ¶¶ 86-90 (November 8, 2001), http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm.

[332] *See* Explanatory Report, Council of Europe, Convention on Cybercrime, ¶¶ 81-85 (November 8, 2001), http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm.

[333] *See,* Explanatory Report, Council of Europe, Convention on Cybercrime, ¶¶ 107-117 (November 8, 2001), http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm.

[334] *See, e.g.,* Gillian Dempsey, *Copyright Guide*, http://www.uq.edu.au/~uqgdemps/copyright.html ("Copyright infringement. . . amounts to theft . . . ."). *See also* The "No Electronic Theft" Act, Pub. L. 105-147, 111 Stat. 2678; 1997 Enacted H.R. 2265; 105 Enacted H.R. 2265, http://www.gseis.ucla.edu/iclp/hr2265.html (amending federal criminal copyright statutes).

[335]Explanatory Report, Council of Europe, Convention on Cybercrime, ¶ 91 (November 8, 2001), http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm.

[336]Explanatory Report, Council of Europe, Convention on Cybercrime, ¶ 93 (November 8, 2001), http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm.

The CISAC Convention is unofficial, the product of a conference held at Stanford University in 1999,[337] but its rather different approach to the development of consensus crimes is still instructive. The provisions of the Convention are to some extent consistent with the propositions set out above, but there are some notable departures.

Like the Council of Europe Convention, the CISAC Convention does not define the crimes as to which it seeks to establish consensus; instead, parties to the Convention agree to "adopt such measures as may be necessary" to criminalize conduct falling into seven offense categories.[338] Specifically, they would agree to criminalize the following: illegal entry into a computer system; manipulating data to disrupt the functioning of a computer system; manipulating data to cause "substantial damage" to persons or property; interfering with computer security measures; manufacturing or distributing a device used to commit an offense defined under the Convention; using computer technology to engage in activity outlawed by a list of treaties; and committing any of the above offenses "with the purpose of targeting the critical infrastructure" of any nation that is a party to the Convention.[339] The drafters of the CISAC Convention did not include provisions directed at computer-related forgery, fraud, theft or conversion because "they are in general already encompassed in extradition treaties".[340]

The first four offense categories are concerned with "new" types of crimes against property: the illegal entry provision requires parties to make computer trespass a crime; the manipulating data provisions require them to make computer-related property damage (damaging a computer system or using a computer system to damage property) a crime; and the evading computer security provision requires parties to criminalize one step in the commission of a computer-trespass/burglary offense.[341] The "computer damage" provision is the first deviation from the propositions set out at the beginning of this section; they, of course, projected that consensus crimes would concentrate on crimes against property and would not focus on crimes involving physical injury to persons.[342] This provision, however, requires parties to define a crime against persons along with a crime against property.[343] Since this is not the only

---

[337] *See* Hoover Institution, Hoover Institution National Security Forum: International Cooperation to Combat Cyber Crime and Terrorism (Dec. 6-7, 1999), http://www-hoover.stanford.edu/research/conferences/bcw99/overview.html. *See also* Center for International Security and Cooperation, A Proposal for an International Convention on Cyber Crime and Terrorism, *supra* note 319.

[338] Instead of attempting to list specific, commonly defined `offenses,' the Stanford Draft refers to types of conduct, and secures commitments from all States Party to enforce any applicable law against every form of covered conduct, or to adopt new laws necessary to create authority to prosecute . . . for such conduct. This approach overcomes the problem of attempting to develop precise, agreed definitions of offenses, and therefore the requirement that every State Party adopt particular formulations as national crimes. *See* CISAC Convention, art. 2, Commentary on the Draft Convention ¶ 1, *available at* http://www.oas.org/juridico/english/monograph.htm. *See also* § II(A)(3), *supra.*

[339] *See* CISAC Convention, art. 3, http://www.oas.org/juridico/english/monograph.htm. Like the Council of Europe's Draft Convention, the CISAC Convention also requires the adoption of legislation imposing liability for aiding and abetting the commission of the identified cybercrimes. *See id*. at Article 4.

[340] *See* CISAC Convention, Commentary on the Draft Convention - § 1 - ¶ 1 (Covered Conduct), http://www.oas.org/juridico/english/monograph.htm. *See also* § II(A)(3), *supra.*

[341] This is a type of inchoate crime. *See* Robbins, *Double Inchoate Crimes, supra,* 26 HARV. J. ON LEGIS. at 24.

[342] *See* § III(B)(1)(A), *supra.*

[343] *See* CISAC Convention, art. 3, http://www.oas.org/juridico/english/monograph.htm.

deviation from what was projected, it is analyzed below, along with the other departures from what was expected.

The fifth offense category is analogous to the "electronic burglary tools" provision included in the Council of Europe's Convention,[344] but the CISAC version sweeps more broadly in that it requires parties to criminalize the manufacture or distribution of devices that can be used to commit *any* crime defined pursuant to the Convention.[345] Like the Council of Europe provision, this offense category is directed at conduct that can facilitate (i.e., aid and abet) the commission of such a crime.[346] But since this provision, like the Council of Europe's version, does not require that the device have been used to commit a crime, it actually imposes both aiding and abetting liability and inchoate liability for attempting-to-aid-and-abet the commission of such a crime.[347] Unlike the Council of Europe's version, this offense category does not impose inchoate liability for the act of acquiring a device as a preparatory step toward committing such a substantive crime.[348] The CISAC provision does require parties to criminalize using such a device to commit a crime defined pursuant to the Convention,[349] which is analogous to making it a crime to use a firearm in the course of committing a felony.[350]

The last two offense categories are unlike anything in the Council of Europe's Convention. The first requires parties to make it a crime to use a computer "as a material factor in committing an act" outlawed by any of several treaties.[351] The treaties impose criminal liability for engaging in specified acts of terrorism, drug trafficking, hostage-taking, aircraft high-jacking and sabotage.[352] Since the treaties already criminalize these acts,[353] this offense category is, like the provision noted in the previous paragraph, analogous to statutes that make it an offense to use a firearm to commit a felony.[354]

---

[344] *See* § III(B)(1), *supra.*

[345] *See* CISAC Convention, art. 3(1)(e), http://www.oas.org/juridico/english/monograph.htm.

[346]*See* CISAC Convention, art. 3(1)(e) (manufacture, sell, post or otherwise distribute "any device or program intended for the purpose of committing any" offense defined pursuant to the Convention), http://www.oas.org/juridico/english/monograph.htm. *See also* § III(B)(1), *supra.*

[347] *See* CISAC Convention, art.3(1)(e), http://www.oas.org/juridico/english/monograph.htm.

[348]*Compare* CISAC Convention, art. 3(1)(e), http://www.oas.org/juridico/english/monograph.htm *with* Council of Europe, Convention on Cybercrime, *supra* note 320, at § 1 – art. 6. *See also* § III(B)(1)(A), *supra.*

[349] *See* CISAC Convention, art. 3(1)(e), http://www.oas.org/juridico/english/monograph.htm.

[350] *See, e.g.,* CONN. GEN. STAT. § 53a-216(a) ("A person is guilty of criminal use of a firearm or electronic defense weapon when he commits any . . . felony . . . and in the commission of such felony he uses or threatens the use of a pistol, revolver, machine gun, shotgun, rifle or other firearm . . . .").

[351] *See* CISAC Convention, art. 3(1)(f), http://www.oas.org/juridico/english/monograph.htm.

[352] *See id.*

[353] *See* Convention on Offenses and Certain Other Acts Committed on Board Aircraft, 20 U.S.T. 2941, art. 1(Sep. 14, 1963) *available at* http://www.iasl.mcgill.ca/airlaw/public/aviation_security/tokyo1963.pdf; Convention for the Suppression of Unlawful Seizure of Aircraft (Hijacking), 22 U.S.T. 1641, art. 1 & 2 (Dec. 16, 1970) *available at* http://www.undcp.org/terrorism_convention_aircraft_seizure.html; Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation (Sabotage), 24 U.S.T. 564, art. 1(Sep. 23, 1971) *available at* http://www.yale.edu/lawweb/avalon/un/civilav.htm; International Convention Against the Taking of Hostages, T.I.A.S. 11081, art. 1(Dec. 17, 1979) *available at*

The final offense category requires parties to make it a crime to commit any of the above offenses "with a purpose of targeting the critical infrastructure of any State Party" to the CISAC Convention.[355] To comply, parties would have to create the separate crime of "using a computer or computer system to commit [one of the specified offenses] for the purpose of attacking the critical infrastructure" of specified nations. This would mean, for example, that someone who uses a device outlawed under the fifth offense category to by-pass computer security measures and illegally gain entry into a computer system to attack the critical infrastructure of a qualifying nation has already committed four crimes under the CISAC Convention. If the offender were to go further and use the computer system to cause "substantial damage" to property, he or she would have committed five crimes under the Convention, and if the damage to property were of a type outlawed by one of the incorporated treaties, the perpetrator would have committed at least six.

This type of layering, or compounding, of liability for a single course of conduct is unusual, found in statutes that attack complex, larger-scale criminal activity.[356] Traditional criminal statutes are based on the premise that it is sufficient to articulate one offense that encompasses a single, sequential course of conduct; complex criminal statutes parse conduct into segments and allow the imposition of liability for each segment.[357]

As this layering of liability indicates, the CISAC Convention is only incidentally concerned with crimes against property or persons, as such; its primary focus is on outlawing the use of computer technology to commit terrorist and terrorist-style acts.[358] Because of that, the provisions of the CISAC

---

http://www.undcp.org/terrorism_convention_hostages.html; International Convention for the Suppression of Terrorist Bombings, 37 I.L.M. 249, art. 2 (Dec. 15, 1997) *available at* http://www.un.org/law/cod/terroris.htm; United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, T.I.A.S., 20 I.L.M. 493, art. 3 (Dec. 20, 1988) *available at* http://www.druglibrary.org/schaffer/legal/un1988nr.htm; International Maritime Organization Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, March 10, 1988, IMO Doc. SUA/CON/15/Rev.1, 1993 Can. T.S. No. 10, art. 3, *available at* http://sedac.ciesin.org/pidb/texts/acrc/unlawfulNav.txt.html.

[354] *See* CISAC Convention, Commentary on the Draft Convention - § 1 -¶ 1 (Covered Conduct), *available at* http://www.oas.org/juridico/english/monograph.htm ("Computers can greatly enhance the potential damage caused by crimes. . . . Therefore, . . . States . . . should be prepared to impose more stringent punishment for the use of cyber capacities in committing the targeted offenses.") .

[355]CISAC Convention, art. 3(1)(g), http://www.oas.org/juridico/english/monograph.htm. The Convention defines "critical infrastructure" as the "networks . . . that provide for timely delivery of government services; medical care; protection . . . by law enforcement; firefighting; food; water; transportation services . . .; supply of energy . . .; financial and banking services and transactions; and information and communications services. . . ." *Id.* at art. 1 - ¶ 7.

[356] *See, e.g.,* Susan W. Brenner, *RICO, CCE and Other Complex Crimes: The Transformation of American Criminal Law?,* 2 WM. & MARY BILL RTS. J. 239, 242-244 (1993).

[357] *See id.*

[358] This focus in apparent in papers presented at the conference. *See, e.g.,* Ariel T. Sobelman, *No Friends—Everyone's an Enemy in Cyberspace????*, Hoover Institution, Hoover Institution National Security Forum: International Cooperation to Combat Cyber Crime and Terrorism (Dec. 6-7, 1999), http://www.oas.org/juridico/english/sobelman.htm (methods used to engage in cybercrime and cyberterrorism are indistinguishable, the difference between the two lying in the effects they aim to achieve).

Convention appear to run counter to the projections that were made earlier in this section; they predicted that consensus crime proposals would concentrate on crimes against property, on child pornography and on obstruction of justice crimes. The CISAC Convention eschews traditional (fraud, forgery, theft, burglary) and non-traditional (copyright infringement) crimes against property, as well as child pornography.[359] The *Commentary* for the Convention explains that the drafters did not address copyright infringement or child pornography because "their inclusion [might] prove controversial."[360] It goes on to note, though, that "a sufficient consensus for including some of these offenses--especially the use of computers for sexual exploitation of minors--may exist", and that offense categories directed at these crimes could be added to the Convention.[361]

The CISAC Convention's focus on terrorism also runs counter to the prediction that terrorism would not be a good candidate for a consensus crime because countries disagree on what "terrorism" is.[362] The drafters of the Convention dealt with this issue in two ways: They built upon a level of existing consensus by incorporating the provisions of treaties that have already defined a variety of terrorist acts.[363] They also expanded upon those definitions by adding computer-related acts directed at "the critical infrastructure" of a signatory party, assuming, perhaps, that nations would find this expansion acceptable because it reaches conduct designed to undermine national integrity.[364]

c. NOTE: THE LIMITS OF PENAL LAW CONSISTENCY

The analysis above--indeed, the notion of consensus crimes--is predicated on the principle that fundamental commonalities exist in the penal laws of every nation because penal law has a common, constant function, namely, to maintain order within a society by prohibiting behaviors that produce socially-intolerable results.[365] A society's inevitable need for this function and the consequent emergence of these commonalities make this principle the logical basis for developing consensus crimes. Unfortunately, it incorporates a qualifying condition that will to some extent limit their acceptance.

---

[359] Neither the CISAC Convention nor the Council of Europe's Draft Convention attempts to develop consensus crimes targeting obstruction of justice offenses. This no doubt reflects empirical reality, e.g., the fact that cybercrimes against property and computer-facilitated child pornography are being committed with ever-increasing frequency, while reported instances of computer-related obstruction of justice are rare.

[360] *See* CISAC Convention, § 1 ¶ 1 (Covered Conduct), http://www.oas.org/juridico/english/monograph.htm.

[361] *Id.*

[362] *See* § III(B)(1), *supra.*

[363] The *Commentary* points out that "most States are parties to these" treaties. *See* CISAC Convention, Commentary on the Draft Convention - § 1 -¶ 1 (Covered Conduct), http://www.oas.org/juridico/english/monograph.htm.

[364] *See generally* Sobelman, *supra* note 358.. The Convention defines "cyber terrorism" as the intentional, unauthorized use or threat to use "violence, disruption or interference against cyber systems, when it is likely that such use would result in death or injury of a person or persons, substantial damage to physical property, civil disorder, or significant economic harm". CISAC Convention, Article 1 - ¶ 2, http://www.oas.org/juridico/english/monograph.htm. This is the only time the term "cyber terrorism" appears in the Convention; it is apparently superseded by the definition of "cyber crime" as "conduct . . . that is classified as an offense . . . by this Convention". *See id.* at Article 1 - ¶ 1.

[365] *See* § III(B)(1), *supra.*

Penal law has evolved to maintain order *within* a society. Each nation-state is concerned with fulfilling its obligations to its citizens (protecting their lives, property and morality) and with ensuring its own survival. As noted earlier, prohibitions barring crimes against persons and property arose because no nation can survive if its citizens are free to prey upon each other.[366] But what if they prey upon citizens of *another* society? What if the citizens of Nation A use cyberspace to prey upon the citizens of Nations B and C? Is this a matter that is likely to be of great concern to Nation A?

There are no ready answers to these questions, but there are historical precedents for this type of behavior that may shed some light on what will ensue in cyberspace. The most analogous of these involve high-seas piracy and intellectual piracy.

High-seas piracy has been around for centuries; indeed, until the seventeenth century it was "widely sanctioned" in most countries, a "national industry."[367] Early in the seventeenth century, the nations of Europe banded together to battle the "infidel" Turkish pirates who had expanded from the Mediterranean into the North Atlantic; by the end of the century, increased trade was transforming attitudes toward piracy.[368] "The advantage to be derived from stealing from one another was giving way to the greater advantage of stable commercial relations."[369] In the eighteenth century, European countries began a war on piracy that included warning other nations "to cease sponsoring pirate expeditions and to crack down on . . . pirates operating . . . from their territories."[370] These efforts were not immediately successful, in part because many non-European nations and even some European colonies resisted, regarding them as unwelcome infringements.[371] This was certainly true in the American colonies, where "business executives and public officials alike continued to provide havens . . . for pirate ships for decades after London ordered a halt to such activities".[372] Piracy therefore persisted well into the nineteenth century; it was not until 1849, for instance, that British forces finally eliminated pirate bases in Crete and Borneo after local rulers refused to act, and pirate havens in the West Indies survived until the 1820s.[373] But by the end of the nineteenth century, piracy had been pretty much eliminated around the

---

[366]This discussion focuses on crimes against persons and property because these are the areas in which there will be the greatest transnational consistency in defining crimes; and the existence of some level of consistency is an essential foundational premise for this analysis. As was explained earlier, there will be diminishing levels of consistency in defining crimes against the state and crimes against morality. *See* § III(B)(1), *supra.*

[367]C.M. SENIOR, A NATION OF PIRATES: ENGLISH PIRACY IN ITS HEYDAY 151 (1976). *See* Ethan A. Nadelmann, *Global Prohibition Regimes,* 44 INTERNATIONAL ORGANIZATION 479-556 (1990), http://www.criminology.fsu.edu/transcrime/articles/GlobalProhibitionRegimes.htm ("Kings . . . and other political magnates . . . viewed piracy as a valued source of wealth and political power").

[368]*See* Nadelmann, *supra* note 367.

[369] *Id.*

[370] *Id.*

[371] *Id.*

[372] *Id.*

[373] *Id.*

world:[374] "As . . . the high seas ceased to be perceived as a no-man's-land, larceny at sea became less justifiable."[375] The prohibition against piracy has been described as the first consensus crime.[376]

High-seas pirates looted tangible property—gold, silver, jewels and other objects. For intangible, intellectual piracy to develop there had to be a means by which intellectual property could be widely produced, marketed and controlled.[377] That process began with the printing press, brought to England in 1476; by 1534, a Crown decree forbade anyone from publishing without a license and approval from royal censors.[378] This measure was meant to promote censorship, not protect property; but by the sixteen century, Britain had begun to protect intellectual property, a process that culminated in the adoption of the first copyright law, the Statute of Anne, in 1709.[379] The statute barred the reproduction of a published work without the copyright owner's consent and shifted ownership of copyrights from publishers to authors.[380] The Statute of Anne is generally considered to have provided the model for modern copyright law "in the Western World";[381] it was widely copied by other countries, including the United States.[382] Its initial effort--the Copyright Act of 1790--gave "citizens" and "residents" the "sole right" to publish their work but did not prohibit importing, selling or publishing works "written . . . or published by any person not a citizen of the United States, in foreign parts".[383] When the Act was adopted, there were no American authors who needed international copyright protection, and this approach - meant to foster the growth of an American publishing industry[384]--let publishers infringe British copyrights "without paying

---

[374] It still survives on a small scale. *See, e.g.,* United Nations, Reports on Piracy: Oceans and the Law of the Sea, Report of the Secretary-General, Fifty-fifth Session, 2000, http://www.geocities.com/Tokyo/Garden/5213/unrep00.htm.

[375] Nadelmann, *supra* note 367.

[376] *Id.*

[377] *See generally* Christophe Kervegant, *Intellectual Property and Electronic Communication,* 10TH BILETA CONFERENCE, 1995, http://www.law.warwick.ac.uk/confs/95-7.html; Debora Halbert, *Computer Technology and Legal Discourse: The Potential for Modern Communication Technology to Challenge Legal Discourses of Authorship and Property,* 1 E LAW (May 1994), http://www.austlii.edu.au/au/other/elaw/v1no2/halbert.html.

[378] *See, e.g.,* Marshall Leaffer, *Protecting Authors' Rights in a Digital Age*, 27 U. TOL. L. REV. 1, 3 (1995).

[379] 8 Anne, c. 19. *See, e.g.,* Lyman Ray Patterson, *The Statute of Anne: Copyright Misconstrued*, 3 HARV. J. ON LEGIS. 223 (1966).

[380] *See, e.g.,* Marshall Leaffer, *supra* note 378*, at* 3; Peter Burger, *The Berne Convention: Its History and Its Key Role in the Future*, 3 J. LAW & TECH. 1, 5 (1988).

[381] *See, e.g.,* Sharon Appel, *Copyright, Digitization Of Images, And Art Museums: Cyberspace and Other New Frontiers*, 6 UCLA ENT. L. REV. 149, 156 (1999).

[382] *See id.* at 156-156 ("It became the model for copyright law in the United States, and is reflected in both the Constitutional provision that authorizes Congress to legislate copyright protection, and the . . . Copyright Act of 1790").

[383] Act of May 31, 1790, ch. 15, 1 Stat. 124, http://www.earlyamerica.com/earlyamerica/firsts/copyright/centinel.jpg.

[384] *See, e.g.,* David G. Post, *Some Thoughts on the Political Economy of Intellectual Property: A Brief Look at the International Copyright Relations of the United States*, Sept. 1998, http://www.temple.edu/lawschool/dpost/Chinapaper.html#N_14_:

royalties to authors from a country against which the United States had just revolted."[385] For a century, American publishers pirated the works of foreign authors, which eventually had an unforeseen result: Pirated works could be sold so cheaply they created a market "that provided high quality foreign books at a price lower than an American author could match."[386] In 1891, the complaints of American authors finally led to the adoption of the Chace Act, which gave non-resident foreign authors copyright protection under American law.[387]

What do these episodes have in common? And if such commonalities exist, what do they reveal about the prospects for achieving transnational consensus on outlawing at least the basic types of cybercrimes against persons and property?

Both episodes involved instances in which societies were willing to allow (or even encourage) their citizens to steal from citizens of other societies. In both, the focus was on crimes against property, not against persons; the motivation was purely economic.[388] In both the conduct took place at the "margins" of the law: high-seas piracy occurred outside the territorial boundaries of any nation and therefore outside the scope of any laws; eighteenth-century American intellectual property piracy occurred at a time when the legal status of intellectual property as "property" was still evolving.[389] Both types of conduct were outlawed when they became economically disadvantageous for the host countries; high-seas piracy was criminalized when it became a threat to the economic advantages derivable from legitimate commerce; and America prohibited intellectual piracy of foreign works when it began to undermine the economic prospects of native authors and the value of domestic intellectual property.[390]

> Simple economics offers a convincing reason why a country . . . might . . . leave foreign works unprotected. As Professor Goldstein puts it, `If Country A imports more literary and artistic works from Country B than it exports to Country B, it will be better off denying protection to works written by Country B's authors even if that means foregoing protection for its own writers in Country B.'. . . Much of the early history of international copyright throughout the West is consistent with this simple principle, as discrimination against foreigners was the rule. . . .

Id. (quoting PAUL GOLDSTEIN, COPYRIGHT'S HIGHWAY: THE LAW AND LORE OF COPYRIGHT FROM GUTENBERG TO THE CELESTIAN JUKEBOX (1994)).

[385]Binyomin Kaplan, Note, *Determining Ownership of Foreign Copyright: A Three-Tier Proposal,* 21 CARDOZO L. REV. 2045, 2050 n. 18 (2000). *See also* Thomas Bender & David Sampliner, *Poets, Pirates, and the Creation of American Literature,* 29 N.Y.U. J. INT'L L. & POL. 255, 256-258 (1996-1997).

[386]Bender & Sampliner, *supra* note 385,at 262.

[387]*See* Act of March 3, 1891, ch. 565, 26 Stat. 1106.

[388] While high-seas piracy was a violent occupation, the infliction of injury and death was incidental to the primary goal of enriching the pirates and/or their sponsors.

[389] *See, e.g.,* Ronald A. Cass, *Copyright, Licensing, and the "First Screen",* 5 MICH. TELECOMM. & TECH. L. REV. 35 (1999), http://www.mttlr.org/volfive/cass.html. *See also* ADAM SMITH, AN INQUIRY INTO THE NATURE AND CAUSES OF THE WEALTH OF NATIONS 330-31 (R. H. Campbell & A. S. Skinner eds, Clarendon Press 1976) (1776).

[390] *See, e.g.,* William W. Fisher III, *The Growth of Intellectual Property: A History of the Ownership of Ideas in the United States,* EIGENTUM IM INTERNATIONALEN VERGLEICH 265-291 (1999), http://www.law.harvard.edu/Academic_Affairs/coursepages/tfisher/iphistory.html. Professor Fisher explains that an important factor in America's willingness to protect foreign works was

One can, therefore, hypothesize that countries may be inclined to tolerate their citizens' victimizing citizens of other nations if (a) the conduct takes place at the "margins" of the law, that is, involves activity that is not definitely proscribed by an applicable set of legal standards and (b) results in a benefit to the victimizing nation. The former gives the victimizing nation at least plausible deniability when confronted with its tolerance of illegal activity; the latter is an obvious motive for tolerating the activity at issue, and may even reinforce the rationale given for tolerating that activity. That is, as to the latter proposition, the victimizing nation may assert, and may believe, that the activity in question is simply a reallocation of scarce resources from a wealthy nation to a poorer nation.

The validity of this hypothesis is examined in Section III(C), *infra*. Before that analysis can proceed, it is necessary to consider the extent to which consensus currently exists as to certain types of cybercrime and the extent to which consensus is likely to be achieved on others. This assessment is contained in the two sections immediately below.[391]

3. EXTENT OF CURRENT CONSENSUS ON CORE CRIMES

> *On the national level, comprehensive and internationally oriented answers to the new challenges of . . . computer crime are often still missing.*[392]

To meet the challenge posed by cybercrime, many countries have reviewed their domestic criminal laws to determine if it is adequate to combat this new phenomenon. Consequently, a number of countries have already amended their criminal laws, including the United States, Austria, Denmark, France, Germany, Greece, Finland, Italy, Turkey, Sweden, Switzerland, Australia, Canada and Japan.[393] And other countries, including Spain, Portugal, the United Kingdom, Malaysia and Singapore have enacted new legislation to prevent computer-related crimes.[394] The sections below describe two surveys of the extent to which consensus appears to have been achieved in outlawing various types of cybercrime.

a. UNAFEI SURVEY

The United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders (UNAFEI) recently surveyed 185 United Nations members as to whether they have "amended their substantive criminal law in order to make it apply to all kind of noxious or otherwise illicit behavior

---

> the transformation of the United States from a net consumer of intellectual property to a net producer. Until approximately the middle of the nineteenth century, more Americans had an interest in `pirating' copyrighted or patented materials produced by foreigners than had an interest in protecting copyrights or patents against `piracy' by foreigners.

[391] *See* §§ III(B)(3)-(4), *infra.*

[392] *Creating a Safer Information Society, supra* note 29, at 9.

[393] *See* § III(A)(2), *supra*. *See also* Appendix, *infra.*

[394] *See* Appendix, *infra*.

that can be committed by means of, through or against computer systems and networks".[395] The questionnaire used in the survey sought information on three categories of cybercrime: (a) the "confidentiality, integrity and availability" crimes, e.g., crimes in which a computer system or data contained within the system is the target of the criminal activity;[396] (b) computer-related fraud and forgery; and (c) pornography and child pornography.[397] Thirty-seven nations replied to the survey.[398]

With regard to the first category of offenses, over 60% of the responding nations indicated that their laws criminalize the unauthorized destruction of computer data, the unauthorized alteration of computer data and unauthorized acts rendering computer data inaccessible to its rightful owners.[399] The criminal law of 51% of the responding countries penalized the unauthorized acquisition of data from a computer system, but in 32% of the responding countries unauthorized acquisition is criminalized only if it is preceded by an act of gaining unauthorized access to a computer system.[400] In 29% of the responding countries, the law draws distinctions between the type of data that is obtained without authorization.[401] France and China, for example, emphasize the protection of data that pertains to national security, state affairs and science and technology, while Spain makes "special reference" to the protection of personal data.[402]

As to computer facilitated fraud and forgery, 62% of the responding countries indicated that their penal laws encompass computer-related fraud.[403] And 43% of the respondents reported that their laws criminalized computer-related forgery.[404]

Finally, 67% of the responding countries indicated that their laws criminalize the use of computer technology to possess and/or distribute pornography, while 70% reported that their laws criminalize the use of such technology to possess or distribute child pornography.[405] The survey found, however, that "in

---

[395] *See* UNAFEI REPORT, OVERVIEW OF THE CRIMINAL LEGISLATION ADDRESSING THE PHENOMENON OF COMPUTER-RELATED CRIME IN THE UNITED NATIONS MEMBER STATES 4 (April 2000), http://www.rechten.vu.nl/~lodder/papers/unafei.html.

[396] These three offenses also provide the basis for the Organization for Economic Cooperation and Development's (OECD) Guidelines for the Security of Information Systems. As such, they are included in most textbooks, legislative acts, and media articles on computer crime. http://www.oecd.org//dsti/sti/it/secur/prod/reg97-2.htm; accessed November 8, 2000.

[397] *See* UNAFEI REPORT, *supra* note 395, at 5.

[398] *Id.* at 4.

[399] *Id.* at 9.

[400] *Id.* at 12.

[401] *Id.* at 12.

[402] *Id.* at 13.

[403] *Id.* at 14.

[404] *Id.* at 14.

[405] *Id.* at 18.

most countries pornographic or pornographic material is not very precisely defined in criminal law."[406] It also found that countries varied in the way their criminal law defined a "child:" for example, in Germany a child is a person "under the age of fourteen years", in Norway a child is anyone under the age of 16 and in Sri Lanka a child is anyone under the age of 18.[407] A number of the countries responding to the survey—including Finland, France and Iceland—have not identified a specific age that defines the outer limits of childhood for the purposes of applying laws criminalizing child pornography.[408]

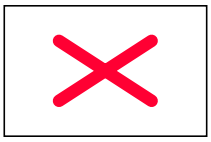
b. AUTHORS' SURVEY

In an effort to determine the extent to which consensus currently exists as to the proscription of cybercrimes, the authors undertook their own survey. They analyzed the cybercrime-specific laws of 50 countries and created a matrix that graphically represents the current state of cybercrime law today.

The matrix—"International Survey of Cybercrime Laws: Consensus Crimes"—looks at eight categories of cybercrime:

- Entering without authority: unauthorized access, hacking, trespass
- Unauthorized destruction, modification, copying or other manipulation of data files;
- Computer sabotage
- Unlawful use of information systems: theft of computer time and use of computer systems to commit traditional crimes such as forgery, terrorism, etc.
- Computer fraud
- Espionage (industrial, national, security, other)
- Breach of privacy
- Damage and/or theft of hardware or software

It concentrates on laws that target crimes against property because—as an earlier section of the article predicted—this is the area where there has been the greatest amount of legislative activity. The matrix appears below.



The matrix shows that - even as to the cybercrime against property which were predicted to be the most immediate source of cybercrime legislation--cybercrime laws are still woefully lacking in Africa, the Middle East, Asia and Oceania. Some South American countries have laws that prohibit some types of cybercrime, but others have essentially no cybercrime law in place. The matrix also shows that technologically advanced countries, especially those in Europe and North America, tend to have cybercrime laws in each of the eight categories set out above; as technological crime becomes an imperative for the remaining nations, most, if not all, will—in accordance with the predictions made earlier in this article—almost certainly replicate what these countries have already done in terms of

[406] *Id.* at 18.

[407] *Id.* at 16.

[408] *Id.* at 16.

adopting cybercrime legislation. What is uncertain is the extent to which countries will then proceed to adopt cybercrime legislation that targets crimes other than those against property; this issue is addressed in Section III(B)(4), *infra.*

4. EXTENT TO WHICH CONSENSUS ON CORE CRIMES IS LIKELY TO BE ACHIEVED

As Section III(B)(1) hypothesized, countries are moving to adopt consensus crimes in certain areas; that section postulated that consensus cybercrimes were the most likely to be adopted with regard to acts targeting property and but were also likely to be adopted to address "new" crimes against persons, online child pornography and new acts intended to obstruct justice. As Section III(B)(3) demonstrated, significant progress has been made toward achieving consensus with regard to outlawing cybercrime against property, and there is also a solid, and growing, consensus on outlawing the use of computers and the Internet to produce and disseminate child pornography. So far, neither crimes against persons nor obstruction of justice activities have been a focal point of the movement toward consensus crimes, but this will change, for the reasons set forth in Section III(B)(1).

There are areas in which consensus will not be achieved. As Section III(B)(1) explained, crimes against morality are the most systemically idiosyncratic types of crime because they are intrinsically bound up with a nation's religious and moral principles. It is true that the essentially-irresistible proliferation of the Internet will lead to some eroding of national moral proscriptions, some leveling in the definitions of crimes against morality, because it is more difficult for nations to maintain stringent standards of moral interdiction when their citizens are exposed to the permissive standards in force elsewhere. Countries have tried to avoid this outcome by restricting or eliminating access to the Internet,[409] but that is likely to prove futile.[410] The effects of this are apparent with regard to gambling, which already enjoys vastly increased legal and social acceptance as a result of online gambling.[411] This does not, of course, mean that a "reverse consensus" will develop which calls for the elimination of crimes against morality; indeed, the opposite will continue to be the case as, for example, online sales of alcohol and/or tobacco find acceptance in some countries but are outlawed in others.[412] The more likely

---

[409] *See, e.g.,* R. Frank Lebowitz, *Internet Cafes Closed in Iran,* DIGITAL FREEDOM NETWORK (May 17, 2001) (Iranian officials closed Internet cafes "`in order to purify materials which go awry of Islamic norms'"). *See also Should Internet Cafes Be Closed?*, BEIJING REVIEW, http://www.bjreview.com.cn/bjreview/EN/Forum/ZM200117.htm (proposals to "ban Internet cafes that operate without a license and severely punish Internet cafes engaged in pornographic activities that disturb social stability" and to eventually outlaw commercial Internet cafes).

[410] *See, e.g.,* Gary R. Bunt, *The Islamic Internet Souq,* Q-NEWS (Nov. 2000), http://www.lamp.ac.uk/cis/liminal/virtuallyislamic/souqnov2000.html ("the Internet is difficult to censor").

[411] *See, e.g.,* Sarah Tippit, *Internet Gambling Grows at Torrid Rate Worldwide,* INFOSEC.COM (May 31, 2000), http://www.info-sec.com/commerce/00/commerce_053100d_j.shtml.

[412] *See, e.g.,* Masaki Hamano, "Introduction", *Comparative Study in the Approach to Jurisdiction in Cyberspace*, http://www.geocities.com/SiliconValley/Bay/6201/intro.html:

> It is technically possible for an alcohol distributor in Japan to sell liquor to people all around the world over the Internet, despite its geographical location. However, most states in the U.S. restrict alcohol sales to government-licensed dealers. On August 3,1999, the House also passed a bill, which allows state attorney generals to go to Federal court to prosecute out-of-state companies that violate state restrictions on alcohol sales. Therefore, it is theoretically possible that an alcohol distributor in Japan be subject to the prosecution for illegal sales of alcohol in America.

outcome is reflected in the matrix which appears at the end of this section; it shows that past efforts to develop consensus crimes have been notably unsuccessful with regard to the articulation of offenses directed at gambling and other crimes against morality.

The same is true of a related area that involves the limitations which are placed on what can be disseminated online. As Section III(B)(3) demonstrated, consensus generally exists as to the imposition of one such limitation, namely, prohibitions on creating, posting and disseminating child pornography, but child pornography seems destined to be a special case.[413] Many countries do, of course, censor what can be posted on the Internet; some make it a crime to post prohibited material.[414] The forms this censorship assumes range from sweeping prohibitions designed to block the dissemination of political statements to narrowly-crafted statutes criminalizing the publication of particular types of material - such as racist/hate speech--on the Internet.[415] Relatively few countries fall into the first category but many outlaw the dissemination of racist/hate speech,[416] which might lead one to assume that consensus could be achieved in this area. Indeed, a provision to this effect was proposed for inclusion in the Council of Europe's Convention on Cyber Crime.[417] Like some other countries, the United States does not, indeed,

---

[413] It is, however, instructive to examine the matrix that appears at the end of this section. It shows that the inclusion of provisions requiring the proscription of computer-facilitated child pornography possession and dissemination were not included in two of the earlier efforts to develop consensus crimes, the OECD effort and the 1999 Council of Europe Draft Convention. A provision to this effect was included only in the most recent version of the Council of Europe Draft Convention.

[414] *See, e.g.,* Tony Taylor, *The Internet: The New Free Speech Battleground,* http://www.cosc.georgetown.edu/~denning/cosc450/papers/taylor.html. *See also* William Yurcik & Zixiang Tan, *The Great (Fire)Wall of China: Internet Security and Information Policy Issues,* TPRC, http://www.tprc.org/abstracts/tan.txt.

[415] *See, e.g.,* Richard S. Rosenberg, *Free Speech on the Internet: Legal. Social and Political Issues,* 9 CSS JOURNAL (July/Sept. 2001), http://www.webcom.com/journal/rosenber.html.

[416] *See, e.g.,* Brendan Fowler, et al., *Can You Yahoo!? The Internet's Digital Fences,* 2001 DUKE L. & TECH. REV. 0012, http://www.law.duke.edu/journals/dltr/articles/2001dltr0012.html.

[417] *See* Racism and Xenophobia in Cyberspace – Motion for a Recommendation, Parliamentary Assembly, Council of Europe (Nov. 7, 2000), http://stars.coe.fr/doc/doc00/EDOC8886.htm (motion calling for including in the Draft Convention on Cyber-Crime a provision defining "as criminal acts the distribution of racist and xenophobic materials, hate speech and racial discrimination on the Internet). *See also* COUNCIL OF EUROPE – PARLIAMENTARY ASSEMBLY, SPRING SESSION (23-27 APRIL 2001), REPORT OF DEBATES OF THE SECOND PART OF THE 2001 ORDINARY SESSION (24 APRIL 2001), http://www.cyber-rights.org/documents/coe_assembly.htm. At this session, the Parliamentary Assembly voted not to include Amendment 1 in the Draft Convention; Amendment 1 would have provided as follows:

> New Article 9 *bis*
>
> RACIAL DISCRIMINATION
>
> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences in accordance with its domestic law the following acts when wilfully committed:
>
> a. producing, offering or making available, distributing or transmitting, procuring or providing, through a computer system, messages of any kind expressing ideas founded on racial superiority or racial hatred, inciting racial discrimination, encouraging racist acts or inciting acts of violence against any race or any group of persons of a different colour or a different ethnic origin;

cannot outlaw the dissemination of hate speech because of the strong protections its law accords free speech Consequently, the attempt to include a prohibition on hate speech in the Convention failed;[418] the matrix appended at the end of this section demonstrates that similar failures plagued an earlier version of the Convention and an effort by the OECD. As this episode demonstrates, consensus will almost certainly not be achieved with regard to content-based restrictions other than those targeting child pornography; and, as Section III(B)(1) explained, prohibitions on child pornography can be distinguished, to some extent at least, from other content-based prohibitions because the primary impetus behind laws against child pornography has traditionally been to address a crime against persons, i.e., the use of children in the production of pornography.[419]

> b. producing, offering or making available, distributing or transmitting, procuring or providing, through a computer system, messages of any kind which negate or condone with a racist or xenophobic intent the crimes defined in Article 6 of the Charter of the International Military Tribunal appended to the London Agreement of 8 August 1945.

[418] *See* EXPLANATORY MEMORANDUM, *supra* note 95, at ¶ 35:

> The committee drafting the Convention discussed the possibility of including other content-related offences, such as the distribution of racist propaganda through computer systems. However, the committee was not in a position to reach consensus on the criminalisation of such conduct. . . . [S]ome delegations expressed strong concern about including such a provision on freedom of expression grounds.

See also COUNCIL OF EUROPE – PARLIAMENTARY ASSEMBLY, SPRING SESSION (23-27 APRIL 2001), REPORT OF DEBATES OF THE SECOND PART OF THE 2001 ORDINARY SESSION (24 APRIL 2001), http://www.cyber-rights.org/documents/coe_assembly.htm. In speaking on the proposal to add a provision criminalizing the dissemination of hate speech, Mr. Jurgens, from the Netherlands, made the following observations:

> I should like to say a few words on the first amendment. I use that expression in two ways. The first amendment of the American Constitution is about free speech, and for our American friends it is one of the bulwarks of their constitutional civilisation. For them, the banning of any type of free speech is difficult to accept. We in Europe have had a different history, and we have had terrible experiences of speech arousing hatred at certain times in the last century. In most European countries, laws have been accepted to ban speech that arouses hatred or racist feeling.
>
> Amendment No. 1 is impeccable and its content is excellent. . . . If free speech is balanced against non-discrimination, it is not always easy to make a decision about which of the two basic rights should be preferred. The Americans prefer free speech to non-discrimination, but we believe that non-discrimination is more important. It is not a matter of us against the Americans: it is more a problem of balancing basic human rights.

See also id., comments of Mr. About of France ("It was disappointing that certain offences had been dropped from the draft convention after pressure from countries, including the United States. The result was inconsistency, since under the revised text it would be allowable to incite racism but not paedophilia").

In February of 2002, the Council of Europe released its protocol on the "criminalisation of acts of a racist or xenophobic nature committed through computer systems". *See* COUNCIL OF EUROPE, COMMITTEE OF EXPERTS ON THE CRIMINALISATION OF ACTS OF A RACIST OR XENOPHOBIC NATURE COMMITTED THROUGH COMPUTER SYSTEMS (February 14, 2002), http://www.treatywatch.org/AvProjetProt2002E.pdf. The protocol was intended to supplement the provisions of the Convention on Cybercrime and to require parties to the Protocol to outlaw the use of computer systems to produce or distribute "racist or xenophobic material". *See id.* at 2-3.

[419] It can also be regarded as a crime against morality. *See* § III(B)(1), *supra.*

Nor will it be achieved with regard to prohibitions targeting online terrorism. The obstacle here is, as Section III(B)(1) explained, the divergent views countries take as to what is and is not a terrorist act. But while the failure to establish consensus crime categories encompassing terrorism *qua* terrorism may let the perpetrators of some terrorist acts avoid prosecution, nations can still pursue and prosecute them for the underlying crimes against persons and crimes against property they commit as part of terrorist agendas.[420]

C. BEYOND CONSENSUS CRIMES

In the networked world, no island is an island.[421]

Section III(B)(3) surveyed the extent to which transnational consensus currently exists as to the proscription of the so-far-identified varieties of cybercrime and found that a rather remarkable degree of consensus is emerging with regard to the core cybercrimes. Section III(B)(4) analyzed the likelihood that transnational consensus will be achieved in proscribing the varieties of cybercrime that exist and that may come to exist and concluded that national variations will continue to exist, especially in some areas.

This postulated lack of consensus will be the product of two mutually-exclusive phenomena: One - which will be the most common of the two - is the *failure* to achieve consensus at the national level, i.e., the failure by some nations to adopt the necessary body of core cybercrime legislation. This failure, in turn, will take at least two forms, one of which is attributable to national variations in the kinds of conduct that are criminally proscribed and in the ways criminal proscriptions are structured. This type of failure is the product of a conscious, intentional act: a country's reviewing its existing laws and affirmatively deciding not to incorporate certain cybercrime prohibitions because they are deemed to be inconsistent with those laws or with the penal philosophy responsible for them. As Section III(B)(4) noted, this type of failure is most likely to occur in areas that have traditionally reflected idiosyncratic national values and concerns, such as the articulation of crimes against morality. One notable example of this type of failure is the United States' refusal to enact laws criminalizing racist/hate speech on the Internet, something many countries regard as an urgent priority.[422] This type of failure is likely to be the least common of the two varieties of failure, at least for the foreseeable future.

The most common type of failure to achieve consensus will be inaction which is attributable to the fact that cybercrime is not an urgent priority for countries where few citizens have access to the Internet.[423] Cybercrime is simply not being addressed in many of the countries around the world; very few of the nations of Africa, the Caribbean and Asia have considered cybercrime as a problem or as a potential problem. In a world where no island is an island, the failure of these nations to address the need for cybercrime legislation may have grave consequences for the rest of the world.

---

[420] *See* § III(B)(1), *supra.*

[421] *Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information*, *supra* note 1.

[422] *See* § III(B)(4), *supra.*

[423] *See, e.g.,* James Evans, *Cyber Laws Emerge, Slowly,* NETWORK WORLD FUSION NEWS (June 30, 2000), http://www.nwfusion.com/news/2000/0630laws.html ("the top 30 industrialized countries are discussing the needs for Internet-specific laws, but it is not the priority in developing countries. The priority in the developing world . . . is just to allow their citizens access the Internet").

Failures to achieve consensus at the national level are unsurprising though still regrettable outcomes; transnational criminal law has, after all, never achieved perfect consensus on real world crimes. But the lack of consensus in outlawing cybercrimes may be the product of a different, rather more unusual phenomenon, namely, the *rejection* of efforts to persuade nations to adopt consistent, comprehensive cybercrime laws. This possibility raises a number of interesting conceptual issues.

The most obvious is the question of why a nation would deliberately reject the notion of adopting cybercrime legislation that would bring it into consensus with the penal laws adopted by other nations. Section III(B)(2)(c) created a framework for answering this question; it derived two propositions from a review of historical instances in which citizens of one nation were allowed to - even encouraged to - prey on citizens of other nations. The propositions are that this type of behavior - which reflects a rejection of criminal proscriptions adopted by at least a subset of the other nations of the world - is most likely to occur: (a) when the conduct at issue exists at the margins of the law, i.e., involves conduct that has not been traditionally criminalized; and (b) when the conduct at issue produces some benefit - an economic benefit or another type of benefit - to the victimizing nation. These propositions can be used to hypothesize "consensus rejection scenarios" that explore the conditions under which nations might deliberately rebuff efforts to achieve consensus in the proscription of cybercrimes. These scenarios are set out below.

Since economic benefits have traditionally been the driver of much criminal behavior, it is only logical to begin by considering how economic benefit might prompt a nation to refuse to proscribe some or all cybercrimes. The most obvious analogy here is to the "bank secrecy" havens that proliferated in the 1980's. Bank secrecy laws became a source of economic benefit for some nations as others, notably the United States, began aggressively tracking the domestic flow of funds in an effort to target money laundering, tax evasion and drug trafficking.[424] Countries discovered that strong bank secrecy laws were a marketable commodity which attracted deposits from those who - for whatever reasons - wished to shield the existence and career of their funds from government scrutiny.[425]

---

[424] *See, e.g.,* Ellen Auwarter, *Compelled Waiver of Bank Secrecy in the Cayman Islands: Solution to International Tax Evasion or Threat to Sovereignty of Nations?*, 9 FORDHAM INT'L680, 680-685 (1985/1986).

[425] *See, e.g.,* Robert J. Mintz, *Swiss Bank Accounts and Bank Secrecy: What You Should Know About Offshore Havens* in ASSET PROTECTION FOR PHYSICIANS AND HIGH-RISK BUSINESS OWNERS (1999), http://www.rjmintz.com/appch10.html:

> The cornerstone product offered by every offshore haven is a legal system that protects against unwanted and unauthorized disclosure of financial matters. Bank secrecy means that, by law, bank employees are prohibited from revealing information concerning a customer's account. This prohibition is buttressed by criminal sanctions including fines and imprisonment.
>
> The mutual goal of the financial institution and the government in the offshore jurisdiction is to protect the confidentiality of the customer's business matters from third party inquiries. Foreign governments, creditors, spouses, and litigants cannot legally obtain information concerning the existence or activity of any
> account.
>
> . . . [E]xisting traditions of individual financial privacy in the Western democracies have yielded to the power of commercial interests, tax authorities, and litigants in a broad variety of civil matters. . . .
>
> Increasingly, the banks assume the role of agents for the government, collecting and feeding information on customers directly to the tax authorities. In Sweden, tax collectors have virtually unlimited access to all personal and financial information of account holders. French and British

How might the derivation of economic benefits lead to the creation of "cybercrime havens"? First of all, nations could derive economic benefits from their haven status in any of several ways: Their citizens and residents might emulate the American copyright pirates of the nineteenth century and illegally appropriate software and other intellectual property belonging to citizens of other nations. Or, the haven states might follow in the footsteps of the bank secrecy and high-seas pirate havens and profit from funds which the cybercriminals deposit and/or expend in their jurisdiction.

One example of this is already emerging: Countries in various parts of the world are competing to encourage online gambling server farms to physically locate within their borders—often by offering to lower the taxes assessed on the casinos[426]--even as they recognize that gambling is illegal in most nations.[427] These countries see online casinos as an excellent source of revenue derivable from the gaming

---

authorities have similar access, and banks must notify officials of the amount of interest earned on an account.

U.S. law requires that financial institutions provide the government with the names and Social Security numbers of account holders. The earnings on every account must be submitted, and copies of every transaction must be retained and made available to those with the proper legal authority.

The laws adopted by the bank secrecy havens do differ from the piracy scenarios analyzed in § III(B)(1)(c) in two important respects: First, the adoption of stringent bank secrecy laws was not, in an of itself, an activity constituting the rejection of otherwise-consistent transnational penal law because laws governing bank secrecy are essentially "neutral" in and of themselves. That is, while laws that impose and/or limit bank secrecy may provide for the imposition of sanctions upon those who violate their provisions, these sanctions are imposed as part of a regulatory scheme and do not define "crimes" in the conventional, penal sense.

The stringent bank secrecy laws adopted by the bank secrecy havens could, of course, be characterized as reflecting an implicit rejection of penal laws adopted in other nations insofar as the application of these laws frustrated the efforts of law enforcement officers to gather evidence of such traditional crimes as tax evasion or drug dealing. Indeed an argument can be made, if one ignores the perquisites of national sovereignty, that the actions of the banks in the secrecy havens made them complicit in the commission of traditional crimes carried out by their depositors; by helping the depositor-perpetrators to conceal evidence of their crimes, the bank secrecy havens aided and abetted their commission of those offenses and/or their escape from prosecution.

Also, stringent bank secrecy laws do not clearly represent an instance in which citizens of haven states are preying upon citizens of nations which require financial institutions to disclose depositor information. It is true that citizens of haven states do profit from the desire of citizens of nations without strong bank secrecy laws to have their financial transactions shielded from disclosure; one can argue that the haven state citizens are indirectly preying upon the misfortunes of citizens of the non-haven states insofar as their bank secrecy laws facilitate activity that is criminal in the non-haven states by frustrating the collection of evidence needed to prosecute offenses such as tax evasion or drug trafficking.

[426] *See, e.g.,* Nelson Rose, *Gambling and the Law: The Future Legal Landscape for Internet Gambling,* FOURTH ANNUAL INTERNET SYMPOSIUM ON INTERNET GAMBLING LAW AND MANAGEMENT (Nov. 2000), http://www.gamblingandthelaw.com/antigua.html (some Australian states are "offering lower tax rates, which range from 8% to a prohibitive 50%. And . . . Norfolk Island offers a 4% tax rate"). *See also* National Centre For Academic Research Into Gaming, Project South Africa – Internet Gaming and South Africa: Implications, Costs, Opportunities 22-23 (August 1999), http://www.gamingtech.com/news/report.doc [hereinafter Project South Africa]

[427] *See, e.g.,* Project South Africa, *supra* note 426 at 7-8.

operations themselves which, as one source noted, represent "earnings which are dollar-based and generated from outside the economy and jurisdiction" which hosts the casino.[428] They also tend to charge those seeking to establish online casinos in their territory exorbitant licensing and application fees that far exceed those assessed for other types of commercial activities.[429] Like the high-seas pirates of the eighteenth century and the American copyright pirates of the nineteenth century, twenty-first century countries that host online casinos realize an economic benefit by letting the casinos prey upon citizens of other nations, nations that have most likely outlawed gambling within their own borders.

A nation might also use its status as a "cybercrime haven" to derive economic benefits in a rather more indirect fashion: The United States pays Israel and Egypt a combined total of $5-6 billion dollars a year to maintain peace,[430] and it gives Colombia, Bolivia and other South American countries hundreds of millions of dollars each year to fight the war on drugs.[431] So it is not difficult to imagine a scenario in which a country approached the United States and said, in effect, "we know our citizens are committing tens of millions in crimes perpetrated against Ebay, Amazon, and other United States interests but, unfortunately, we do not have the expertise needed to stop this activity. If you give us millions (or even billions) of dollars in support we will make an effort to do so." The country would be using its status as a cybercrime haven to extort an economic benefit from the United States and/or other nations that were being victimized by the activities of its citizens and/or residents.

How might a nation go about becoming a "cybercrime haven"? It could do so by design or by default.

As to default, many of the former Soviet Republics are already major cybercrime havens already--de facto havens, not de jure.[432] Their status as cybercrime havens results not only from what is often an absence of penal law that can be used to prosecute cybercrime activity but also from a paucity of cybercrime investigative experience and expertise, technical knowledge and forensic and computer hardware.[433] These countries also decline to assist law enforcement officials seeking to apprehend

---

[428] *See, e.g.,* Project South Africa, *supra* note 426, at 9.

[429] *See, e.g.,* Project South Africa, *supra* note 426, at 23 (recommending that online casinos should be charged a US $50,000 application fee, a US $350,000 first-year license fee and a US $100,000 annual license fee).

[430] *See, e.g.,* Hamdesa Tuso, *Constructed on a Sand Foundation: The Crisis of U.S. Foreign Policy Toward the Horn of Africa During the Post Cold War Era – A Critical Review,* Part III, http://www.sidamaconcern.com/articles/us_policy3.html.

[431] *See, e.g., The Effective National Drug Control Strategy 1999*, http://www.csdp.org/edcs/page47.htm; Steven Wisotsky, *A Society of Suspects: The War on Drugs and Civil Liberties,* POLICY ANALYSIS (Oct. 2, 1992), http://www.cato.org/pubs/pas/pa-180.html.

[432] *See, e.g.,* Mike Brunker, *Cyberspace Evidence Seizure Upheld,* MSNBC (May 30, 2001), http://stacks.msnbc.com/news/563379.asp ("Eastern Europe and nations of the former Soviet Union have become a hotbed in recent years for computer crime aimed at businesses in the United States and other Western nations").

[433] *See, e.g.,* Frank J. Ciluffo & Robert J. Johnson, *Corruption in the Kremlin,* INTERNATIONAL POLICE REVIEW (Sept./Oct. 1997), reprinted by Global Organized Crime Project, http://www.csis.org/goc/ao971001.html:

> Russian law enforcement agencies are easily being outspent by organized crime groups in acquiring the best computer personnel and equipment. We need to ensure Russia has the equipment and training it needs to prevent the country from becoming a safe haven for cyber-criminals.

cybercriminals operating within their borders; in one recent case Russian authorities repeatedly ignored FBI requests for assistance in apprehending Russian hackers who were breaking into the computers of U.S. companies as part of an ongoing extortion scam.[434]

As to design, there are several ways this could be done: A nation desiring to become a cybercrime "extradition haven" might simply refuse to execute extradition treaties encompassing the commission of cybercrimes. It might direct its law enforcement officials not to cooperate with officials from other countries who were trying to secure evidence pertaining the commission of cybercrimes against citizens of those countries. Or it might frustrate the application of extradition treaties by refusing to outlaw some or all cybercrimes.[435] Or the haven country might exploit definitional problems, i.e., even though a treaty might be in force between Countries X and Y that provided for the extradition of those who commit economic crimes such as financial fraud, when asked to extradite certain persons Country Y could decline on the grounds that their activity constituted a cybercrime, not a financial fraud, and was therefore outside the scope of the treaty. A more imaginative approach would be for the haven state to set up an arrangement which lets cybercriminals who are physically located either in the haven state or elsewhere vector their criminal activities through the haven state in such a way that they are untraceable. This would effectively render their activities immune from the investigative efforts of law enforcement officials located in other countries. Pragmatically, this would be as effective as the non-extradition of offenders located within the haven state but it would also let the haven state extend its shield to encompass the activities of non-resident cybercriminals. In a sense, this is already happening; countries that do not keep log files or require their Internet Service Providers to do so effectively frustrate all cybercrime investigations because the perpetrator of a cybercrime cannot be traced back to a given IP address or machine.

The rise of cyberspace, of course, means that a crime haven no longer needs to be a conventional, land-based sovereignty. A haven might be a "virtual country," and virtual countries have already been created.[436] A ship on the high seas or a platform built five hundred miles off the coast of Australia could be a server farm that evades current legal regimes while hosting cybercrime activities. Or the haven might be an airborne server farm that carried out a variety of network instructions while hovering over international waters; a great deal of illegal material could be switched and sent, and before the plane landed all hard drives could be erased and wiped so that forensics recovery was impossible.

What kinds of non-economic benefit might prompt a nation to become a "cybercrime haven"? The most obvious, of course, is the realization of some political benefit; the most likely scenario here would be for a country to shelter the activities of terrorists who use computer technology to carry out their activities. If the haven state's motivations were purely non-economic, it might shield terrorism activities out of a sense of loyalty, of identification with the terrorist group's agenda. Of course, the haven state could also act out of mixed motives, at once sympathizing with the terrorist group's agenda and profiting from the terrorist group's presence and/or from hosting its cyber-terrorist activity.

---

[434] *See, e.g.,* Brunker, *supra* note 432 ("Eastern Europe and nations of the former Soviet Union have become a hotbed in recent years for computer crime aimed at businesses in the United States and other Western nations").

[435] An extradition haven would almost certainly have to outlaw certain types of cybercrimes, such as hacking, cyber-theft and cyber-extortion, to protect its own citizens from the depredations of cybercriminals. It might, however, craft these prohibitions so that they did not encompass acts committed within the haven state's territory but that were directed at citizens of other nations.

[436] *See, e.g.,* Bertil Lintner, *Cyberfraud – The Fictitious "Domain of Melchizedek",* http://www.infowar.com/law/99/law_060299a_j.shtml

One can postulate yet another scenario in which a country becomes a cybercrime haven for other than economic reasons: a country - like the United States - which has strong laws protecting freedom of expression can become a haven for those who wish to express views that are outlawed elsewhere in the world. Because of its strong First Amendment protections for free speech, the United States is, in a sense, a haven for those who create and maintain web sites that disseminate hate speech, racist views, Nazi and Neo-Nazi philosophies and other viewpoints the expression of which are outlawed by other nations.[437]

This notion that a country can be a "cybercrime speech haven" implicates the second proposition set out in Section III(B)(2)(c), namely, that a country is more likely to host illegal activity, which may involve letting its citizens prey on citizens of other countries, when the activity at issue exists on the margins of the law, i.e., has not been traditionally defined as a "crime." This is certainly true of the racist/hate speech laws that are found in some nations but that would be unconstitutional in the United States; it can also be true, at least to some extent, of cyberterrorism activities since, as Section III(B)(1) explained, there is some disagreement at the transnational level as to what does, and does not, constitute "terrorism." The definition of political offenses and of crimes against morality tends to be more idiosyncratic than the definition of crimes against persons and crimes against property,[438] which means that a haven state's conduct with regard to activities falling into the first two categories may not be so clearly regarded as tolerating or even facilitating illegal conduct as would conduct pertaining to crimes against persons or crimes against property.

Why is this important? It is important because it gives the haven state plausible deniability. If, say, a nation refused to sign a cybercrime *extradition* treaty in order to set itself up as a cybercrime haven, it would no doubt prefer to predicate its refusal on some at least ostensibly neutral principle, such as the argument that the offenses encompassed by the treaty were not "crimes" under its historical penal law. If such a nation were take an indirect approach to becoming a cybercrime haven - such as allowing cybercriminals to vector their activities through facilities it maintained - it might prefer to be able to claim ignorance as to the criminality of the activities at issue.

---

[437]This outcome illustrates the fluidity of the categories developed in § III(B)(1), *supra.* That discussion postulated that crimes are divisible into four categories: crimes against persons; crimes against property; crimes against the state; and crimes against morality. In the United States, the dissemination of hate speech is regarded as a victimless crime, and victimless crimes tend to be classified as crimes against morality. Section III(B)(1) postulated that it would be very difficult to achieve consensus with regard to crimes against morality, so if one regards the dissemination of hate speech as a crime against morality the outcome noted above seems neither surprising nor egregious. Citizens of other countries, however, do not regard the dissemination of hate speech as a victimless crime but as a crime against persons. *See, e.g.,* David Pred, *Two Countries, Two Victimless Crimes*, UNIVERSITEIT UTRECHT http://www.law.uu.nl/rt/rsoc/DavidPred.pdf. The outcome noted above becomes much more shocking when it is construed in this light.

[438] *See* § III(B)(1), *supra.*

IV. CONCLUSION

Cybercrime presents the nations of the world with a problem they have never before had to address, i.e., the permeability of national borders. As long as crime remained a "real world" phenomenon which required the commission of some overt act or omission which, by definition, had a circumscribed geographical reach, localized, idiosyncratic criminal laws were sufficient to protect a nation's citizens from those who would do them harm.

It is true, of course, that the rise of modern transportation - planes, trains, ships and automobiles - made it possible for criminals to commit offenses in one country and then flee to another. Nations responded to this phenomenon by developing extradition treaties which allowed the country in which a miscreant took refuge to hand him or her off to the country whose citizens had been victimized, as long as certain conditions--notably the proscription of the conduct at issue by both countries--were met. The requirement of dual criminality was seldom an obstacle under these extradition regimes - until recently - because the crimes at issue were "real world" crimes and, as Section III(B)(1) demonstrated, there are basic commonalities in the structure of penal codes developed to deal with "real world" behaviors.

As the "Love Bug" episode demonstrated, the varieties of cybercrime can make the operation of these regimes problematic. The obstacle that barred efforts to prosecute the accused architect of the "Love Bug" in any of the countries that were victimized by his efforts was inadvertent, the Philippines' unintentional failure to have adopted even the most basic of cybercrime prohibitions. If future "Love Bug" episodes are to be avoided, countries must work together to devise a set of core consensus crimes that can be used to pursue cybercriminals wherever they may operate.

APPENDIX: SURVEY OF CYBERCRIME-SPECIFIC LEGISLATION[439]

This section surveys the extent to which countries have adopted legislation that specifically targets the commission of computer-related crime.[440] It does not attempt to analyze the extent to which a country's traditional penal legislation can be applied to prosecute those who use computer technology to commit such traditional offenses as theft, fraud and forgery.[441]

I. WESTERN EUROPE

Austria

Austria's Privacy Act 2000, which into effect on January 1, 2000, establishes penalties for unlawful acts directed at data.[442] Specifically, it provides that a fine shall be assessed for doing any of the

---

[439]The authors gratefully acknowledge the invaluable contributions made by Kimberly L. Bruce and Adam M. Savino, both students at the University of Dayton School of Law. Ms. Bruce and Mr. Savino spent many hours researching the state of cybercrime laws in various countries, especially those for which information was not readily available through conventional sources. Their energy, resourcefulness and creativity markedly enhanced the comprehensiveness and accuracy of this survey.

[440]Some, notably EURIM – The European Information Society Group, take the view that there

> are few new e-crimes. It is essential to separate the crime from the method by which it is committed. Computers increase criminal productivity as effectively as commercial efficiency – and reduce the risk of being caught. . . . Ill-conceived legislation is being heavily promoted although it fails to address the real issues, such as electronically assisted fraud, impersonation and theft, while creating unrealistic demands on industry to support law enforcement in areas where the costs, responsibilities and liabilities have not been thought through. . . .

EURIM, EURIM Briefing No. 34 (April 2002), http://www.eurim.org/briefings/BR34.htm. *See also infra* note 441.

[441]Conventional penal legislation can be used to prosecute cybercrime. A United Nations-sponsored survey conducted in 2000 asked countries if their extant penal codes could be used to prosecute computer-facilitated fraud and forgery. *See* H.W.K. Kaspersen & A.R. Lodder, *Overview of the Criminal Legislation Addressing the Phenomenon of Computer- related in the United Nations Member States*, 4-5, Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, April 15, 2000, http://www.rechten.vu.nl/~lodder/papers/unafei.pdf. Thirty-seven countries from around the world plus a non-governmental authority from Australia responded to the questionnaire. *See id.* at 3. Their responses showed that "[i]n the criminal law of 62% of the countries, the offences of `fraudulent obtaining' - like fraud, embezzlement or other fraudulent acts to obtain goods, money or other financial gains - apply in a functionally equivalent manner to the computer environment" and that "[i] In the criminal law of 43% of the countries, forgery offences apply, in a functionally equivalent manner, to the computer records or files, as they do in the paper environment." *Id.* at 14.

[442] Schjolberg, *supra* note 164.

following: (1) willfully obtaining or maintaining unlawful access to a data application; (2) intentionally transmitting data in violation of the Data Secrecy Clause, especially if he or she was given access to it for other purposes; (3) using data contrary to a legal judgment or decision, failing to correct false data or failing to delete data; and (4) intentionally deleting data.[443]

Belgium

In November, 200, the Belgian Parliament adopted new legislation which would insert a series of new articles, which deal with computer crime, into the Belgian Criminal Code.[444] The articles make "computer forgery, computer fraud, hacking and sabotage . . . criminal offences in their own right".[445]

Belgium's approach to computer forgery—defined by new Article 210(b) of the Criminal Code--differs from that taken elsewhere:[446] "Instead of conferring the quality of `a written document' upon data stored in a computer system," the new article creates the distinct crime of computer forgery, which consists of "the falsification of computerised information."[447] The new offense does not "require the particular intention of pecuniary gain or intention to cause harm" because these acts are covered by the new articles on fraud and sabotage.[448] It encompasses the completed act or the attempt to "`intentionally hide the truth by means of computerised manipulations of legally pertinent data, or the use of such

---

[443] *Id*.

[444] *See* Martin Donaghy, Stanbrook & Hooper, INTERNATIONAL CENTRE FOR COMMERCIAL LAW, http://www.icclaw.com/devs/belgium/it/beit_004.htm; Schjolberg, *supra* note 164.

[445] Donaghy, Stanbrook & Hooper, *supra* note 444.

[446] *Id*. Article 210(b) of the Criminal Code provides as follows:

> §1. The author of a forgery who, by introducing into a computer system, or by modifying or deleting data which is stored, processed or transmitted by a computer system, or by modifying, by any technological means, the possible utilisation of data within a computer system, thereby modifies the legal effect of such data, may be sentenced to a term of imprisonment of 6 months to 5 years and a fine of [BFr5,200-20m], or to one of these sentences.
>
> §2. The user of data so obtained, knowing that it is false, may be sentenced in the same way as the author of the forgery.
>
> §3. The attempt to commit the offence provided in §1 may be sanctioned by a sentence of imprisonment of 6 months to 3 years and to a fine of [BFr5,200-10m] or to one of these sentences.
>
> §4. The sentences carried by §§1-3 are doubled if an offence to one of these provisions is committed within 5 years of a judgment or decision of condemnation for one of these offences [or for computer fraud, hacking, sabotage or illegal interception of telecommunications.

[447] *Id*.

[448] *Id*.

data'".[449] The forgery or attempted forgery must cause "the modification of the legal effect of such data."[450]

Unlike the forgery offense, the new computer fraud offense—codified in Article 504(4)—requires that the "computerised manipulations have procured . . . a fraudulent pecuniary advantage" for the perpetrator or someone else.[451] The computer sabotage offense—codified as Article 550(3)--requires that the perpetrator act with the intent to cause harm.[452] It fills what had been a gap in Belgian criminal law:

---

[449] *Id*.

[450] *Id*.

[451] *Id.* Article 504(4) provides as follows:

> §1. Any person who procures for himself or for others a fraudulent pecuniary advantage, by introducing into a computer system, or by modifying or deleting data which is stored, processed or transmitted by a computer system, or by modifying, by any technological means, the possible utilisation of data within a computer system, may be sentenced to a term of imprisonment of 6 months to 5 years and to a fine of [BFr5,200-20m] or to one of these sentences.
>
> §2. The attempt to commit the offence specified in §1 may be sanctioned by a term of imprisonment of 6 months to 3 years and to a fine of [BFr5,200-10m] or to one of these sentences.
>
> §3. The sentences carried by §§ 1 and 2 are doubled if an offence under one of these provisions is committed within 5 years of a judgment or decision of condemnation for one of these offences [or for computer forgery, hacking, sabotage or illegal interception of telecommunications.

Id.

[452] *Id.* Article 550(3) provides as follows:

> §1. Any person who, with the intention to cause harm, directly or indirectly, introduces into, modifies or deletes data within a computer system, or who modifies by any other technological means the possible utilisation of data within a computer system, may be sentenced to a term of imprisonment of 6 months to 3 years and to a fine of [BFr5,200-5m] or to one of these sentences.
>
> §2. Any person who, following the commission of an offence specified in §1, causes damage to the data in the computer system concerned, or in any other computer system, may be sentenced to a term of imprisonment of 6 months to 5 years and to a fine of [BFr5,200-15m] or to one of these sentences.
>
> §3. Any person who, following the commission of an offence specified in §1, impedes, totally or partially, the correct functioning of the computer system concerned, or any other computer system, may be sentenced to a term of imprisonment of 1 year to 5 years and to a fine of [BFr5,200-20m] or to one of these sentences.
>
> §4. Any person who, with the intention to defraud or with the intention to cause harm, creates, supplies, diffuses or commercialises data which is stored, processed or transmitted by means of a computer system, when he is aware that this data may be used to damage other data or impede the correct functioning of a computer system, may be sentenced to a term of imprisonment of 6 months to 3 years and to a fine of [BFr5,200-20m] or to one of these sentences.

> In the past, the notion of sabotage required the destruction or damage of physical objects. The destruction or damage of computerised data is not covered by the existing Criminal Code. The new article therefore criminalises any manipulation of data with the intent to cause harm. [453]

If the data manipulation causes damage to the computer system or affects its functioning, the behavior is punished more severely than simply causing damage to data. [454] "Impeding the correct functioning of a computer system is now . . . considered as causing damage." [455] The new offense can also be used to prosecute "those who create or spread viruses, or who create programmes which create viruses." [456]

Finally, the new hacking provision penalizes "both internal and external hacking", e.g., both the acts of breaking into a computer system from outside and that of exceeding one's lawful access to a computer system.[457] "No particular intention is required of an external hacker . . . (although the intention

---

> §5. The sentences carried by §§1-4 are doubled if an offence under one of these provisions is committed within 5 years of a judgment or decision of condemnation for one of these offences [or for computer fraud, forgery, hacking or illegal interception of telecommunications].

Id.

[453] *Id*.

[454] *Id*.

[455] *Id*.

[456] *Id*. *See* Article 550(3) § 4, *supra*.

[457] *Id.* Article 550(b) provides as follows:

> §1. Any person who, aware that he is not authorised, accesses or maintains his access to a computer system, may be sentenced to a term of imprisonment of 3 months to 1 year and to a fine of [BFr5,200-20m] or to one of these sentences.
>
> If the offence specified in §1 above is committed with intention to defraud, the term of imprisonment may be from 6 months to 2 years.
>
> §2. Any person who, with the intention to defraud or with the intention to cause harm, exceeds his power of access to a computer system, may be sentenced to a term of imprisonment of 6 months to 2 years and to a fine of [BFr5,200-20m] or to one of these sentences.
>
> §3. Any person finding himself in one of the situations specified in §§1 and 2 and who either:
>
> 1. accesses data which is stored, processed or transmitted by a computer system, or procures such data in any way whatsoever, or
>
> 2. makes any use whatsoever of a computer system, or
>
> 3. causes any damage, even unintentionally, to a computer system or to data which is stored, processed or transmitted by such a system,may be sentenced to a term of imprisonment of 1 to 3 years and to a fine of [BFr5,200-10m] or to one of these sentences.
>
> §4. The attempt to commit one of the offences specified in §§ 1 and 2 is sanctioned by the same sentences as the offence itself.

to defraud is an aggravating circumstance), whereas the activities of the internal hacker must be motivated by a fraudulent intention or an intention to cause harm in order to be sanctioned."[458] The article also makes it a crime to attempt to break into a computer system. [459]

Denmark

Section 263(2) of the Danish Criminal Code makes it an offense to, "in an unlawful manner," obtain "access to another person's information or programs which are meant to be used in a data processing system". [460] The basic sanction is imprisonment "for a term not exceeding 6 months", but if the offense is committed with the intent to "procure or make oneself acquainted with information concerning trade secrets of a company or under other extraordinary aggravating circumstances," the penalty is increased to "imprisonment for a term not exceeding 2 years." [461]

Section 279 of the Danish Penal Code outlaws using a computer to commit fraud.[462] Specifically, it declares that anyone who, "for the purpose of obtaining for himself or for others an unlawful gain" unlawfully alters, adds or erases "information or programs for the use of electronic data processing, or who in any other manner attempts to affect the results of such data processing" is guilty of computer fraud. [463] The basic sanction is imprisonment for up to "one year and six months", but the penalty can be

---

> §5. Any person who, with the intention to defraud or with the intention to cause harm, seeks, assembles, supplies, diffuses or commercialises data which is stored, processed or transmitted by a computer system and by means of which the offences specified in §§1-4 may be committed, may be sentenced to a term of imprisonment of 6 months to 3 years and to a fine of [BFr5,200-20m] or to one of these sentences.
>
> §6. Any person who orders or incites one of the offences specified in §§ 1-5 to be committed may be sentenced to a term of imprisonment of 6 months to 5 years and to a fine of [BFr5,200-40m] or to one of these sentences.
>
> §7. Any person who, aware that data has been obtained by the commission of one of the offences specified in §§1-3, holds, reveals or divulges to another person, or makes any use whatsoever of data thus obtained, may be sentenced to a term of imprisonment of 6 months to 3 years and to a fine of [BFr5,200-20m] or to one of these sentences.
>
> §8. The sentences carried by §§1-7 are doubled if an offence under one of these provisions is committed within 5 years of a judgment or decision of condemnation for one of these offences [or for computer fraud, forgery, sabotage or illegal interception of telecommunications].

Id.

[458] *Id.*

[459] *Id.*

[460] Schjolberg, *supra* note 164.

[461] *Id*.

[462] McConnell International, *Cyber Security Legislation*, http://www.mcconnellinternational.com/services/Updatedlaws.htm.

[463] *Id*.

increased—to as much as eight years imprisonment—when the crime was of "a particularly aggravated nature" or where the perpetrator committed "a large number of such offences".[464]

Two provisions of the Danish Criminal Code can be used to prosecute someone who uses a computer to cause damage. Section 193(1) is essentially an anti-terrorism provision, making it a crime unlawfully to cause "major disturbances in the operation of public means of communication, of the public mail service, of publicly used telegraph or telephone services, of radio and television installations, of data processing systems or of installations for the public supply of water, gas, electricity or heating". The offense is punishable with imprisonment for up to four years; if mitigating circumstances are shown or if the offense was committed through negligence, the penalty is reduced to a fine or "simple detention".[465] Section 291(1) makes it a crime to destroy, damage or remove "objects belonging to others".[466] The basic penalty is a fine or imprisonment for up to one year, but if the damage is "very serious" and the perpetrator has previous convictions for similar acts, the sanction can be increased to imprisonment for up to four years.[467]

Finland

Finland outlaws the creation and dissemination of computer viruses under the aegis of an offense called "criminal computer mischief."[468] It has also criminalized computer fraud[469] and damage to

[464] Danish Criminal Code §§ 285 & 286(1), McConnell International, *Cyber Security Legislation*, http://www.mcconnellinternational.com/services/Updatedlaws.htm.

[465] *Id*. §§ 193(1) & 193(2).

[466] *Id*. § 291(1).

[467] *Id*. §§ 291(1) & 291(2).

[468] Finnish Penal Code, Chapter 34 § 9a, ENLIST, http://www.urova.fi/home/oiffi/enlist/resources/penal.html:

> A person who, in order to cause harm to automatic data processing or the functioning of a data system or telecommunications system,
>
> > (1) produces or makes available a computer program or set of programming instructions designed to cause harm to automatic data processing or the functioning of a data system or telecommunications system or to damage the data or software contained in such a system, or distributes such a program or set of instructions, or
> >
> > (2) makes available guidelines for the production of a computer program or set of programming instructions or distributes such guidelines,
>
> shall be sentenced, unless an equally severe or more severe penalty for the act is provided elsewhere in the law, for criminal computer mischief to a fine or to imprisonment for at most two years.

[469] *Id*. Chapter 36 § 1(2). The statute makes it a crime for someone who, acting with the purpose of obtaining an unlawful financial benefit for himself or herself or in order to cause harm to another, enters false data into a computer or otherwise interferes with "automatic data processing" thereby falsifying "the end result of data processing and in this way causes another person economic loss." *Id.*

computer data.[470] It also enacted an omnibus provision entitled "data and communications offenses" which outlaws hacking and the interception of electronic communications, among other activities.[471]

[470] *Id*. Chapter 35 § 2 ("a person who, in order to cause damage to another, unjustifiably destroys, defaces, conceals or hides data recorded on an information device or other recording shall be sentenced for criminal damage").

[471] *Id*. Chapter 38:

> Section 1 - *Secrecy offence* (578/1995)
>
> A person who in violation of a secrecy obligation provided by an Act or Decree or specifically ordered by an authority by virtue of an Act
>
> (1) discloses information which should be kept secret and which he/she has learnt by virtue of his/her position or task or in the performance of a duty; or
>
> (2) makes use of such a secret for the gain of himself/herself or another
>
> shall be sentenced, unless the act is punishable under chapter 40, section 5, for a *secrecy offence* to a fine or to imprisonment for at most one year.
>
> Section 2 - *Secrecy violation* (578/1995)
>
> (1) If the secrecy offence, in view of the significance of the act as concerns the protection of privacy or confidentiality, or the other relevant circumstances, is petty when assessed as a whole, the offender shall be sentenced for a *secrecy violation* to a fine.
>
> (2) A person shall also be sentenced for a secrecy violation if he/she has violated a secrecy obligation referred to in section 1 and it is specifically provided that such violation is punishable as secrecy violation.
>
> Section 3 - *Message interception* (578/1995)
>
> (1) A person who unlawfully
>
> (1) opens a letter or another closed communication addressed to another or hacks into the contents of an electronic or other technically recorded message which is protected from outsiders;
>
> (2) eavesdrops using a special technical device or secretly records the speech of another using a technical device, so that the speech listened to or recorded is not intended to come into his/her knowledge or the knowledge of other outsiders, and the circumstances are such that the person speaking has had no reason to believe that he/she is being overheard; or
>
> (3) obtains information on the contents of a call, telegram, transmission of text, images or data, or another comparable telemessage or on the transmission or reception of such a message
>
> shall be sentenced for *message interception* to a fine or to imprisonment for at most one year.
>
> (2) An attempt is punishable.
>
> Section 4 - *Aggravated message interception* (578/1995)
>
> (1) If in the message interception
>
> (1) the offender commits the offence by making use of his/her position in the service of a telecommunications company, as referred in the Act on the Protection of Privacy and Data Protection in Telecommunications (565/1999) or his/her other special position of trust; (567/1999)

(2) the offender commits the offence by making use of a computer program or special technical device designed or altered for such purpose, or otherwise especially methodically; or

(3) the message that is the object of the offence has an especially confidential content or the act constitutes a grave violation of the protection of privacy

and the message interception is aggravated also when assessed as a whole, the offender shall be sentenced for *aggravated message interception* to imprisonment for at most three years.
(2) An attempt is punishable.

Section 5 - *Interference* (578/1995)

A person who by tampering with the operation of a device used in postal, telecommunications or radio traffic, by mischievously transmitting interfering messages over radio or telecommunications channels or in another comparable manner unlawfully hinders or interferes with postal, telecommunications or radio traffic, shall be sentenced for *interference* to a fine or to imprisonment for at most two years.

Section 6 - *Aggravated interference* (578/1995)

If in the interference

(1) the offender commits the offence by making use of his/her position in the service of an institution referred to in the Telecommunications Act, a cable operator referred to in the Cable Transmission Act (307/1987) or a public broadcasting institution, or his/her other special position of trust;

(2) the offence hinders or interferes with the radio transmission of distress signals or such other telecommunications or radio transmissions that are made in order to protect human life

and the interference is aggravated also when assessed as a whole, the offender shall be sentenced for *aggravated interference* to imprisonment for at least four months and at most four years.

Section 7 - *Petty interference* (578/1995)

If the interference, in view of its nature or extent or the other circumstances of the offence, is of minor significance when assessed as a whole, the offender shall be sentenced for *petty interference* to a fine.

Section 8 - *Computer break-in* (578/1995)

(1) A person who by using an unauthorised access code or by otherwise breaking a protection unlawfully hacks into a computer system where data is processed, stored or transmitted electronically or in a corresponding technical manner, or into a separately protected part of such a system, shall be sentenced for a *computer break-in* to a fine or to imprisonment for at most one year.

(2) A person shall also be sentenced for a computer break-in if he, without hacking into the computer system or a part thereof, by using a special technical device unlawfully obtains information contained in a computer system referred to in (1).

(3) An attempt is punishable.

(4) This section applies only to acts that are not subject to an equally severe or more severe penalty provided elsewhere in the law.

Section 9 - *Data protection offence* (525/1999)

A person who deliberately or grossly negligently

France

France has outlawed hacking and cracking since 1993.[472]

Germany

Germany has criminalized computer sabotage[473] and computer fraud, [474] along with data theft[475] and data alteration or destruction. [476]

---

(1) processes personal data in violation of the provisions of the Personal Data Act (523/1999) on the exclusivity of purpose, the general prerequisites for processing, the necessity and integrity of processing, sensitive data, identification codes or the processing of personal data for specific purposes;

(2) by giving false or misleading information prevents or attempts to prevent a data subject from using his/her right of inspection; or

(3) conveys personal data to states outside the European Union or the European Economic Area in violation of chapter 5 of the Personal Data Act,

and thereby violates the privacy of the data subject or causes him/her other damage or significant inconvenience, shall be sentenced for a *data protection offence* to a fine or to imprisonment for at most one year.

See also id. Chapter 49.

[472]*See* Schjolberg, *supra* note 164:

Chapter III: ATTACKS ON SYSTEMS FOR AUTOMATED DATA PROCESSING

Article 323-1:

The act of fraudulently gaining access to, or maintaining, in all or part of an automated data processing system is punishable by imprisonment not exceeding one year and a fine of up to 100.000 F.

Whenever this results in the suppression or modification of data contained in the system, or an alteration in the functioning of the system, the act is punished by imprisonment not exceeding two years and a fine up to 200.000 FF.

Article 323-2:

The act of hindering or of distorting the functioning of an automated data processing system is punishable by imprisonment not exceeding three years and a fine up to 300.000 FF.

Article 323-3:

The act of fraudulently introducing data into an automated data processing system or of fraudulently suppressing or modifying data contained therein is punishable by imprisonment not exceeding three years and a fine up to 300.000 FF.

See also Code Pénal, Livre III, titre II, chapitre IlI, Article 323, http://www.rabenou.org/penal/L3.html#art323-1.

Greece

The Greek Penal Code "protects 'secrecy' and punishes everyone, who unlawfully copies, prints, uses, discloses to a third party, or by any means violates secret data or computer programs." [477] It also criminalizes unauthorized access to computer systems and computer programs, as well as and computer fraud. [478]

Iceland

Iceland has criminalized unlawfully obtaining access to data or to programs stored as data.[479]

Ireland

Section 2(1) of the Criminal Damage Act makes it an offence for anyone to damage property belonging to another or to be reckless as to whether such property would be damaged.[480] Section 5 of the

---

[473] *See* German Penal Code § 303b, http://www.bmj.bund.de/publik/e_stgb.pdf:

> (1) Whoever interferes with data processing which is of substantial significance to the business or enterprise of another or a public authority by:
>
> 1. committing an act under Section303a subsection (1); or
> 2. destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier,
>
> shall be punished with imprisonment for not more than five years or a fine.
>
> (2) An attempt shall be punishable.

[474] *See id*. § 263a(1) ("Whoever, with the intent of obtaining for himself or a third person an unlawful material benefit, damages the assets of another by influencing the result of a data processing operation through incorrect configuration of a program, use of incorrect or incomplete data, unauthorized use of data or other unauthorized influence on the order of events, shall be punished with imprisonment for not more than five years or a fine").

[475] *See id*. § 202a(1) ("Whoever, without authorization, obtains data for himself or another, which was not intended for him and was specially protected against unauthorized access, shall be punished with imprisonment for not more than three years or a fine").

[476] *See id*. § 303a(1) ("Whoever unlawfully deletes, suppresses, renders unusable or alters data (Section 202a subsection (2)), shall be punished with imprisonment for not more than two years or a fine").

[477] *Issues Facing the Secure Links of CoCs: Derived Legal Issues*, COSACC CONSORTIUM, http://cosacc.acci.gr/d3_1/doc0015.htm (citing Greek Penal Code Article 370B).

[478] *Id.* (citing Greek Penal Code Article 370C and Article 386A). *See* Schjolberg, *supra* note 164, at Article 370C § 2.

[479] Schjolberg, *supra* note 164 (citing Iceland Penal Code § 228(1)).

[480] *Protecting Your Business from Computer Misuse*, LK SHIELDS, SOLICITORS, http://www.lkshields.ie/newsletters/issue5.htm.

Act makes it a crime for someone to operate a computer "without lawful excuse" (a) "within the State with intent to access any data kept either within or outside the State" or (b) "outside the State with intent to access any data kept within the State".[481] Such a person commits the offense regardless of "whether or not he accesses any data".[482] This provision also encompasses the dissemination of viruses.[483] Curiously, the Act nowhere defines "computer", though it does define "data" as "`information in a form in which it can be accessed by means of a computer and includes a program'".[484]

Italy

Article 615.5 of the Italian Penal Code makes it a crime to disseminate programs aimed at damaging or interrupting the operations of a computer system.[485] Article 615 also criminalizes hacking and the unlawful possession and distribution of computer access codes.[486]

> It is possible that computer hackers might claim that any damage they cause is unintentional, but it is still likely that their actions would be viewed as reckless for entering a computer system without consent. This arguably comes within the meaning of 'reckless' in the Act.

Id.

[481] Schjolberg, *supra* note 164.

[482] *Id*.

[483] *Protecting Your Business from Computer Misuse*, *supra* note 480:

> Viruses also come under this section. While it might be difficult to prove that a virus in a computer system caused any real damage, it could also be argued that the mere introduction of a virus is an offence since the Act defines 'damage' as including 'addition to' data.

[484] *Id.*

[485] *See* Italian Penal Code, Article 615.5, http://www.ladysharrow.ndirect.co.uk/library/laws/italian_law.htm:

> Anyone who spreads, transmits or delivers to computer program, whether written by himself or by someone else, aimed at or having the effect of damaging to computer or telecommunication system, the programs or given contained in or pertaining to it, or interrupting in full or in part or disrupting its operation is punished with the imprisonment for to term of up to two years and to aim of up to It. L. 20.000.000.

[486] *See, e.g.,* Schjolberg, *supra* note 164:

> Penal Code Article 615 ter: Unauthorized access into a computer or telecommunication systems:
>
> Anyone who enters unauthorized into a computer or telecommunication system protected by security measures, or remains in it against the expressed or implied will of the one who has the right to exclude him, shall be sentenced to imprisonment not exceeding three years.
>
> The imprisonment is from one until five years:
>
> 1) if the crime is committed by a public official or by an officer of a public service, through abuse of power or through violation of the duties concerning the function or the service, or by a person

Luxembourg

Luxembourg makes it an offense either to fraudulently gain access to a computer system or to alter, suppress or modify data contained in such a system. [487]

Malta

On January 8, 2001, the Parliament enacted the Electronic Commerce Act, which adds a new section, entitled "Computer Misuse", to the Maltese Criminal Code.[488] Aside from definitional and procedural provisions, the new Computer Misuse section of the Criminal Code creates offenses falling into two categories, unlawful access to information[489] and misuse of hardware. [490]

> who practices - even without a licence - the profession of a private investigator, or with abuse of the capacity of a system operator.
>
> 2) if to commit the crime the culprit uses violence upon things or people, or if he is manifestedly armed.
>
> 3) if the deed causes the destruction or the damage of the system or the partial or total interruption of its working, or rather the destruction or damage of the data, the information or the programs contained in it.
>
> Should the deeds of the 1st and 2nd paragraphs concern computer or telecommunication systems of military interest or (concerning) public order or public security or civil defence or whatsoever public interest, the penalty is - respectively- one to five years or three to eight years' imprisonment. In the case provided for in the 1st paragraph, the crime is liable to punishment only after an action by the plaintiff; the other cases are prosecutioned "ex-officio".
>
> -615 quater: Illegal Possession and Diffusion of Access Codes to Computer or Telecommunication Systems:
>
> Whoever, in order to obtain a profit for himself or for another or to cause damage to others, illegally gets hold of, reproduces, propagates, transmits or deliver codes, key-words or other means for the access to a computer or telecommunication system protected by safety measures, or however provides information or instructions fit to the above purpose, is punished with the imprisonment not exceeding one year and a fine not exceeding 10 million liras.
>
> The penalty is imprisonment from one until two years and a fine from 10 until 20 million liras in the case of one of the circumstances numbered in 1 and 2 in the 4th paragraph of article 617-quater.
>
> with imprisonment not exceeding two years and fined not exceeding 20 million liras.

[487] *See, e.g.,* Schjolberg, *supra* note 164 (citing Act of July 15th, 1993, Article 509-1).

[488] *See* Government of Malta, Electronic Commerce Act, Act III of 2001, http://cimu.magnet.mt/whitepapers/ecommerceact.pdf.

[489] *Id. at* § 337(C)(1):

> A person who without authorization does any of the following acts shall be guilty of an offence against this article –

The Netherlands

The Netherlands has outlawed hacking.[491]

(a) uses a computer or any other device or equipment to access any data, software or supporting documentation held in that computer or on any other computer, or uses, copies or modifies any such data, software or supporting documentation;

(b) outputs any data, software or supporting documentation from the computer in which it is held, whether by having it displayed or in any other manner whatsoever;

(c) copies any data, software or supporting documentation to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

(d) prevents or hinders access to any data, software or supporting documentation;

(e) impairs the operation of any system, software or the integrity or reliability of any data;

(f) takes possession of or makes use of any data, software or supporting documentation;

(g) installs, moves, alters, erases, destroys, varies or adds to any data, software or supporting documentation;

(h) discloses a password or any other means of access, access code or other access information to any unauthorised person;

(i) uses another person's access code, password, user name, electronic mail address or other means of access or identification information in a computer;

(j) discloses any data, software or supporting documentation unless this is required in the course of his duties or by any other law.

[490] *See id*. § 337(D):

Any person who without authorization does any of the following acts shall be guilty of an offence against this article –

(a) modifies computer equipment or supplies that are used or intended to be used in a computer, computer system or computer network;

(b) takes possession of, damages or destroys a computer, computer system, computer network, or computer supplies used or intended to be used in a computer, computer system or computer network or impairs the operation of any of the aforesaid.

[491] *See, e.g.,* Schjolberg, *supra* note 164:

Any person who intentionally and unlawfully accesses an automated system for the storage or processing of data, or part of such a system, shall be liable, as guilty of breach of computer peace, to term of imprisonment not exceeding six months or a fine of 10.000 guilders if he:

(a). Breaks through a security system, or

Norway

Norway has outlawed hacking and a form of cyberterrorism.[492]

Portugal

Portugal has outlawed hacking, which becomes an aggravated offense if the perpetrator obtains information by violating security measures or obtains access to trade secrets or other information protected by law.[493]

Spain

Spain has criminalized the interception of e-mail or "any other communications signal" and the copying, use or modificaton of "private personal or family data of another individual".[494] Spain has also outlawed computer fraud and the unauthorized use of telecommunications terminal equipment.[495]

Sweden

Sweden has made "data trespass" a crime.[496]

(b). obtains access by a technical intervention, with the help of false signals or a false key or by acting in a false capacity.

(citing Netherlands Criminal Code Article 138A).

[492] *See, e.g.,* Schjolberg, *supra* note 164 (citing Norway Penal Code § 145 & § 151 b).

[493] *See, e.g., id*. (citing Criminal Information Law of August 17, 1991).

[494]*See* Spanish Penal Code, Article 197, McConnell International, *Cyber Security Legislation*, http://www.mcconnellinternational.com/services/Updatedlaws.htm.

[495]*See id.*

Article 248.

1. Any individual will be guilty of fraud who, with intent to profit, uses sufficient deceit to cause another individual to err, inducing him or her to commit an act of disposition to the detriment of him or herself or a third party.
2. Also guilty of fraud will be any individual who, with intent to profit and using computer manipulation or any similar contrivance, causes the unauthorized transfer of any personal asset to the detriment of a third party.

Article 256.

Any individual who makes use of any telecommunications terminal equipment without the consent of the owner thereof, causing damage to the latter in excess of fifty thousand pesetas, will be subject to punishment consisting of a fine of between three and twelve months [sic].

Switzerland

Article 143(a) of the Swiss Penal Code makes hacking a crime.[497]

United Kingdom

The centerpiece of the United Kingdom's approach to cybercrime is the Computer Misuse Act of 1990.[498] The Act creates three distinct offenses: unauthorized access to computer material;[499]

---

[496] *See* Section 21 of The Data Act 1973 (as amended with effect from January 1, 1989), http://elj.warwick.ac.uk/jilt/dp/material/dataact.htm:

> Any person who unlawfully procures access to a recording for automatic data processing or who unlawfully alters or deletes or inserts such a recording in a file shall be sentenced for data trespass to a fine or to imprisonment not exceeding two years, unless the offence is punishable under the Penal Code. Equivalent to a recording in a file is, in this respect, information being transmitted by electronic or similar means to be used in automatic data processing.
>
> Any person who attempts or prepares a data trespass crime shall be sentenced in accordance with the Penal Code, Chapter 23. Should the infraction, if accomplished, be considered as only an offence, the perpetrator must be sentenced in accordance with this paragraph.

[497] *See* Schjolberg, *supra* note 164:

> Anyone, who without authorization, and without the intent of procuring an unlawful gain, accesses a data processing system which are specially protected against unauthorized access, by electronic devices, shall be sentenced to imprisonment or fines.

[498] *See* Computer Misuse Act 1990 (c. 18) (Eng.), http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm.

[499] *See id*. § 1:

> (1) A person is guilty of an offence if—
>
> (a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;
> (b) the access he intends to secure is unauthorised; and
> (c) he knows at the time when he causes the computer to perform the function that that is the case.
>
> (2) The intent a person has to have to commit an offence under this section need not be directed at—
>
> (a) any particular program or data;
> (b) a program or data of any particular kind; or
> (c) a program or data held in any particular computer.
>
> (3) A person guilty of an offence under this section shall be liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both.

unauthorized access with intent to commit or facilitate commission of further offenses;[500] and unauthorized modification of computer material.[501] Like Ireland's Criminal Damage Act, described

---

[500] *See id*. § 2:

> (1) A person is guilty of an offence under this section if he commits an offence under section 1 above . . . with intent—
>
> (a) to commit an offence to which this section applies; or
> (b) to facilitate the commission of such an offence (whether by himself or by any other person); and the offence he intends to commit or facilitate is referred to below in this section as the further offence.
>
> (2) This section applies to offences—
>
> (a) for which the sentence is fixed by law; or
> (b) for which a person of twenty-one years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the [1980 c. 43.] Magistrates' Courts Act 1980).
>
> (3) It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion.
>
> (4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.
>
> (5) A person guilty of an offence under this section shall be liable—
>
> (a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and
> (b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

[501] *See id*. § 3:

> (1) A person is guilty of an offence if—
>
> (a) he does any act which causes an unauthorised modification of the contents of any computer; and
> (b) at the time when he does the act he has the requisite intent and the requisite knowledge.
>
> (2) For the purposes of subsection (1)(b) above the requisite intent is an intent to cause a modification of the contents of any computer and by so doing—
>
> (a) to impair the operation of any computer;
> (b) to prevent or hinder access to any program or data held in any computer; or
> (c) to impair the operation of any such program or the reliability of any such data.
>
> (3) The intent need not be directed at—
>
> (a) any particular computer;
> (b) any particular program or data or a program or data of any particular kind; or
> (c) any particular modification or a modification of any particular kind.

above, the Computer Misuse Act makes no effort to define "computer", [502] though it does define "access." [503] One criticism leveled at the Computer Misuse Act is that it needs to be revised, since it "takes not account of the Internet, and has not yet been updated to cover offences such as denial of service (DOS) attacks."[504]

II. RUSSIA AND EASTERN EUROPE

Countries of Central and Eastern Europe have generally made less progress in reforming their legal systems to incorporate cybercrime, though Russia stands as an exception. Russia has developed an

---

> (4) For the purposes of subsection (1)(b) above the requisite knowledge is knowledge that any modification he intends to cause is unauthorised.
>
> (5) It is immaterial for the purposes of this section whether an unauthorised modification or any intended effect of it of a kind mentioned in subsection (2) above is, or is intended to be, permanent or merely temporary.
>
> (6) For the purposes of the [1971 c. 48.] Criminal Damage Act 1971 a modification of the contents of a computer shall not be regarded as damaging any computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition.
>
> (7) A person guilty of an offence under this section shall be liable—
>
> (a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and
> (b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

[502] *See, e.g.,* Dennis Jackson, *Computers, Crimes, and British Justice*, http://www.ja.net/CERT/Jackson/Computers_and_Justice.txt:

> The Computer Misuse Act makes no attempt to define what is a computer. This is deliberate. When the act was drafted it was recognised that it would be impossible to predict the form of computer systems five, ten, or twenty years into the future. The simple approach was taken; in the absence of a definition within the act then the ordinary, every day, meaning of a computer would be used by the courts.
>
> The same approach had already been taken by several other acts. It is accepted that the term `computer' is now an ordinary word in the English language which can be construed by the judge.

(footnotes omitted).

[503] *See* Computer Misuse Act 1990 (c. 18) (Eng.), § 17, http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm.

[504] Madeline Bennett, *High-Tech Vigilantes Face Legal Threat*, ZDNET UK, May 8, 2001, http://news.zdnet.co.uk/story/0,,s2086068,00.html.

extensive legal framework to detect, punish, and prevent computer crime, but implementation remains problematic. Other countries of Central and Eastern Europe have also started addressing cybercrime as part of the larger on-going legal reforms in the region. Romania and Poland have draft laws underway that include computer-related provisions.

Albania

A study published in December of 2000 found that Albania had no cybercrime specific laws in place.[505] It noted, however, that the Albanian Authority for the Regulation of Telecommunications had begun discussions "on the topic of cyber laws, with the goal of preparing protocols of collaboration and exchanging information."[506]

Bosnia

The Federation of Bosnia and Herzegovina has implemented an article in their criminal code to criminalize computer data theft.[507] Article 193(2) of the Criminal Code, which went into effect on November 20, 1998, makes it illegal to break into a computer database containing personal data, use such data, or make such information available to another person.[508]

Bulgaria

The Bulgarian criminal code has established crimes involving computers in two separate categories; crimes against intellectual property and general economic crimes.[509] Article 172a, which covers crimes against intellectual property, criminalizes reproducing or distributing another's property without the copyright holders consent.[510] The punishment for this type of crime is imprisonment of up to three years and a fine from 1000,00-3000,00 levas, however, if the crime is a second offense or causes substantial harm, the punishment is up to five years imprisonment and a fine of 3000,00-5000,00 levas.[511]

---

[505] *See Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information*, *supra* note 1. No cybercrime provisions appear in Albania's Criminal Code. *See* Criminal Code of the Republic of Albania, http://pbosnia.kentlaw.edu/resources/legal/albania/crim_code.htm.

[506] *See Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information, supra* note 1.

[507] http://www.ohr.int/ohr-dept/legal/crim-codes/default.asp?content_id=5130

[508] *Id.* Article 193(2) reads as follows:

> (2) Whoever without authorization breaks into a computer data base containing personal data or makes them available to another, shall be punished by imprisonment for a term not exceeding six months.

[509] http://www.aippi.org/reports/q169/q169_bulgaria_e.html.

[510] *Id.* Article 172a:

1. Recording, reproducing, distributing, broadcasting or transmitting with technical means or using in another way another's object of science, literature or art without the required by the law consent of the holder of the copyright.
2. Recording, reproducing, distributing, broadcasting or transmitting with technical means or using in another way of sound record, video record or radio program, TV program, software or computer program without the required by law consent of the holder of the respective right.

[511] *Id.*

Under general economic crimes in the criminal code, Article 227 forbids using a mark, industrial design, or topology of integrated circuits in commercial activities.[512] The punishment for this crime is imprisonment of up to three years and a fine of up to 5000,00 levas.[513]

Czech Republic

In 1999, the Ministry of the Interior of the Czech Republic issued a report that surveyed cybercrime analyzed the adequacy of the legislation available to combat it. In the paragraph below, the report discusses "crime in information technology" and notes the extent to which is can be pursued using existing law:

> **Hacking in IT and programmes**
>
> § 152 of the Criminal Code - Infringement of copyright
> § 182 of the Criminal Code - Impairing and endangering the operation of public utility facilities
> § 249 of the Criminal Code - Unauthorised use of other people's articles
> § 257a of the Criminal Code - Damaging and misusing records in information stores
>
> Unlawful conduct in the **electronics trade**
>
> § 121 of the Criminal Code - Harming the consumer
> § 127 of the Criminal Code - Breaching the binding regulations of economic relations
> § 128 of the Criminal Code - Misuse of information in business relations
> § 250 of the Criminal Code – Fraud[514]

The report emphasizes that cybercrime can also "involve e.g. vice crimes, certain crimes against the Republic and the security of the Republic, and other crimes, especially economic ones."[515] And it explains that various entities are working to develop legislation which will target other areas of cybercrime.[516]

Estonia

Estonia recently adopted legislation outlawing computer fraud, sabotage and related offenses.[517] The computer fraud provision makes it a crime to receive "proprietary benefits through entry,

---

[512] *Id.* Article 227:
1. Use in commercial activities of a mark, industrial design, or topology of integrated circuits.

[513] *Id.*

[514] Czech Republic, Ministry of the Interior, *Conception of the Fight Against Intellectual Property Crime*, § 2.2.1(b), http://www.mvcr.cz/ (footnotes omitted).

[515] *Id*.

[516] *Id*.

[517] *See* Estonian Penal Code §§ 206-208, http://www.legaltext.ee/en/andmebaas/ava.asp?m=026. *See* also McConnell International, *Cyber Security Legislation*, http://www.mcconnellinternational.com/services/Updatedlaws.htm.

replacement, deletion or blocking of computer programs or data" which "influences the result of the data processing operation.[518] The computer sabotage provision makes the "[u]nlawful replacement, deletion, damaging or blocking of data or programs in a computer" and/or the "unlawful entry of data or programs in a computer" a crime if "significant damage is thereby caused".[519] Another provision makes it illegal to disseminate computer viruses; the basic punishment is a fine or up to one year's imprisonment, but if the offense is repeated or is committed "in a manner which causes significant damage" the allowable period of imprisonment rises to three years.[520] Another provision makes it ulawful to damage or block computer network connections.[521] It is also illegal to distribute "the protection codes of a computer, computer system or computer network, if committed for the purpose of personal gain and in a manner which causes significant damage or results in other serious consequences."[522]

Hungary

So far, Hungary's only cybercrime-specific penal legislation is a provision criminalizing computer fraud.[523]

Latvia

Latvia has outlawed the following: "arbitrarily accessing computer systems;"[524] the unauthorized acquisition of computer software;[525] damaging computer software;[526] disseminating a computer virus;[527] and violating "safety provisions regarding information systems."[528]

---

[518] *See* Estonian Penal Code § 213, http://www.legaltext.ee/en/andmebaas/ava.asp?m=026 (punishable by fine or incarceration for up to five years).

[519] *See id.* § 206(1) (punishable by fine or incarceration for up to one year). If the offense is committed "with the intention to interfere with the work of a computer or a telecommunications system," it is punishable by a fine or incarceration for up to three years. *See id.* § 206(2).

[520] *See id.* §208.

[521] *See id.* § 207. Both are punishable by fine or imprisonment for up to two years. *Id.*

[522] *See id.* § 284. The sanctions are a fine or imprisonment for up to three years.

[523] *See* Hungary, Penal Code Penal Code § 300C(1), Schjolberg, *supra* note 164:

> Whoever, with the intent of obtaining for himself an unlawful gain, or by damaging, interferes with the results of electronic data processing, by altering programs, by erasing, by entering incorrect or incomplete data, or by other unlawful means commits an offence, imprisonment for a term not exceeding 3 years may be imposed.

See also id. § 300C(3) ("Whoever commits the offences under subsection (1)-(2) by using an electronic card for public or mobile telephone, or by altering the microprogram for the mobile telephone commits also fraud in connection with data").

[524] *See* Latvia, The Criminal Law § 241, http://www.ttc.lv/en/default-translations-lr.htm:

> (1) For a person who commits arbitrarily accessing an automated computer system, if opportunity for an outsider to acquire the information entered into the system is caused thereby, the applicable sentence is custodial arrest, or a fine not exceeding eighty times the minimum monthly wage.

Poland

The Polish Penal Code criminalizes the following: unauthorized access to information;[529] damaging, destroying or deleting information; [530] and destroying, deleting or altering information "having

---

(2) For a person who commits the same acts, if breaching of computer software protective systems or accessing of communications lines is associated therewith, the applicable sentence is deprivation of liberty for a term not exceeding one year, or a fine not exceeding one hundred and fifty times the minimum monthly wage.

[525] *See id*. § 242:

(1) For a person who commits unauthorised copying of computer software, files or databases stored in the memory of a computer system, if substantial harm is caused thereby, the applicable sentence is custodial arrest, or a fine not exceeding eighty times the minimum monthly wage. For a person who commits the same acts, if commission thereof is repeated or breaching of computer software protection systems or accessing of communications lines is associated therewith, the applicable sentence is deprivation of liberty for a term not exceeding two years, or a fine not exceeding one hundred and fifty times the minimum monthly wage.

[526] *See id*. § 243:

For a person who commits modifying, altering, damaging or destroying, without authorisation, information stored in an automated computer-based system, or knowingly entering false information into an automated system, or knowingly damaging or destroying information bearing devices, computer software or protection systems, if substantial harm is caused thereby, the applicable sentence is deprivation of liberty for a term not exceeding five years, or a fine not exceeding one hundred and fifty times the minimum monthly wage.

[527] *See id*. § 244:

(1) For a person who commits disseminating a computer virus, that is, the disseminating knowingly of such means of programming as causes unsanctioned destruction or alteration of computer software or information, or damages information equipment, or destroys protection systems, or who commits introduction of a new kind of virus into the computer software environment, the applicable sentence is deprivation of liberty for a term not exceeding four years, or a fine not exceeding two hundred times the minimum monthly wage.
(2) For a person who commits the same acts, if substantial harm is caused thereby, the applicable sentence is deprivation of liberty for a term not exceeding ten years.

[528] *See id*. § 245:

For a person who commits violation of provisions regarding information storage and processing, which have been formulated in accordance with an information system or the protection thereof, or violation of other safety provisions regarding computerised information systems, where committed by a person responsible for compliance with these provisions, if such has been a cause of theft, destruction or damage of the information, or other substantial harm has been caused thereby, the applicable sentence is deprivation of liberty for a term not exceeding two years, or community service, or a fine not exceeding forty times the minimum monthly wage.

[529] *See* Penal Code of Poland Article 267(1), Schjolberg, *supra* note 164 ("Whoever, without being authorised to do so, aquires information not destined for him, by opening a sealed letter, or connecting to a wire that transmits information or by breaching electronic, magnetic or other special protection . . . shall be subject to a fine, the . . .

a particular significance for national defense, transport safety, [or] operation of the government". [531] Other provisions make it a crime to connect to a computer network to gather information for the benefit of a foreign intelligence service[532] and to interfere with the automatic processing, gathering or transfer of information. [533] Finally, Poland also criminalizes improper access to and/or use of personal information,[534] as well as the act of failing to protect such data when one is under an obligation to do so. [535]

Romania

The Romanian Criminal Code contains no special legislation on computer crimes. Several years ago, the government drafted "The Code for Information Technologies Development and Use." The draft Code stipulated that "IT offenses" would be punishable by imprisonment for terms ranging from two to ten years, depending on the offense and its severity. The offenses include: unauthorized access to an information system for the capture, storage, processing and distribution of data and/or programs or for altering, damaging and destroying hardware, data and/or software; data embezzlement, program disturbance, alteration and erroneous data transmission resulting in data flow disturbance; and computer fraud. An accidental entry into data flows that caused any of the above-mentioned types of damage would be criminalized if the perpetrator did not immediately acknowledge the act to the Romanian Authority for Informatics. Infringements, such as disobeying the recommendations or authorizations of Romanian Authority for Informatics, would be punished by fines.[536] The Code for Information Technologies Development and Use was submitted to the European Commission, with comments received in March of 1998.[537] The second revised Code was approved by the Government and forwarded to the Romanian Parliament in 1999, but Parliament has so far not acted upon it. [538]

---

restriction of liberty or . . . deprivation of liberty for up to 2 years"). *See also* McConnell International, *Cyber Security Legislation - Poland*, http://www.mcconnellinternational.com/services/Updatedlaws.htm.

[530] *See* Penal Code of Poland Article 268(1), Schjolberg, *supra* note 164 ("Whoever, not being . . . authorised to do so, destroys, damages, deletes or alters a record of essential information or otherwise prevents or makes it significantly difficult for an authorised person to obtain knowledge of that information, shall be subject to" a fine or imprisonment for up to two years). *See also id*. 268(2) ("If the act specified in § 1 concerns the record on an electronic information carrier, the perpetrator shall be subject to the . . . deprivation of liberty for up to 3 years").

[531] *See id*. 269(1).

[532] *See* Poland Penal Code, Article 130(3), McConnell International, *Cyber Security Legislation - Poland*, http://www.mcconnellinternational.com/services/Updatedlaws.htm.

[533] *See id*. 130(4).

[534] *See* Poland Data Protection Act, Articles 49 & 50, McConnell International, *Cyber Security Legislation - Poland*, http://www.mcconnellinternational.com/services/Updatedlaws.htm.

[535] *See id*. at Article 51.

[536] Draft Law, "The Code for Information Technologies Development and Use," The Parliament of Romania, The Chamber of Deputies, The Senate, URL:http://info.cni.ro/legeng.htm#t1.

[537] *See Romania: Legislation and Regulation*, EUROPEMEDIA.NET, June 25, 2001, http://www.europemedia.net/showfactfile.asp?FactFileID=4&FactID=C28.

[538] *See id.*

Russia

Prior to 1997, the Criminal Code of the Russian Federation included no specific provisions regarding computer crimes. The new Penal Code of the Russian Federation, which entered into force in 1997, directly addresses computer crimes. Chapter 28 of this Code is entitled "Crimes in the Domain of Computerized Information" and includes articles on unauthorized access to computerized information;[539] the creation, use, and promulgation of harmful computer software; [540] and breach of operating rules for computers, computer systems and networks. [541]

---

[539] *See* Penal Code of the Russian Federation, June 13, 1996, Chapter 28, Article 272, http://www.elspa.ru/Laws/uk_e.htm:

> 1. Unwarranted access to computer information protected by the law that is information on a computer carrier, in a computer, a computer system, or their network, if such actions has resulted in destruction, blocking, modification or copying of information, disruption in the operation of a computer, a computer system or a network thereof, -shall be punishable with a fine in the amount of two hundred to five hundred minimum wages or in the amount of wages or other income of the convict during a period from two to five months, or corrective labor for a term from six months to one year, or imprisonment for up to two years.
>
> 2. The same action committed by a group of persons who have previously conspired or by an organized group, or by a person using his office, or equally having an access to a computer, a computer system or a network thereof,
> shall be punishable with a fine in the amount of five hundred to eight hundred minimum wages or in the amount of wages or other income of the convict during a period from five to eight months, or corrective labor for a term from one to two years, or arrest for a term from three to six months, or imprisonment for up to five years.

[540] *See id*. at Article 273:

> 1. Creation of computer software or introducing of changes in the existing software which are known to result in unwarranted destruction, blocking, modification or copying of information, disruption in the operation of a computer, a computer system or a network thereof, or equally the use or distribution of such software or computer carriers with such software, shall be publishable with imprisonment for a term of up to three years with a fine in the amount from two hundred to five hundred minimum wages or in the amount of wages or other income of the convict during the period from two to five months.
>
> 2. The same actions which have led to grave consequences out of carelessness,
> shall be punishable with three to seven years in prison.

[541] *See id*. at Article 274:

> 1. Violation of computer, computer system or computer network operating rules by a person having an access to a computer, a computer system or a network thereof, which resulted in the destruction, blocking or modification of legally protected computer information, if such action caused material damage, shall be punishable with a ban on holding certain positions or engaging in certain activities for a term of up to five years, or compulsory labor during a period from one hundred and eighty to two hundred and forty hours, or restriction of freedom for up to two years.
>
> 2. The same action which caused grave consequences as a result of carelessness, -shall be punishable with up to four years in prison.

Slovenia

There is no special legislation dealing with computer crime in force in Slovenia.[542] Slovenia expects to ratify the Convention on Cybercrime soon, which would obligate it to prosecute the offenses specified by the Convention.[543] The Slovene Penal Code generally enables the prosecution of all the offenses listed in the Convention,[544] though small amendments may be necessary to ensure full compliance with the Convention.[545] Greater amendments will likely to bring the Slovene Criminal Procedure Code into compliance with the Convention.[546]

Yugoslavia

Yugoslavia has enacted several laws attempting to address cyber crimes. These include laws on the information system of the government agencies and organization of FRY ("Official Gazette of FRY" No.59/98) and laws on the protection of personal data ("Official Gazette of FRY", No. 24/98).[547]

III. NORTH AMERICA

Canada

Canada criminalizes a number of computer-related offenses, including computer mischief;[548] data theft;[549] invasion of privacy;[550] computer fraud;[551] and hacking/cracking and virus dissemination.[552]

---

[542]Email from Klemen Tièar to Kimberly Bruce (May 27, 2002) (on file with the authors).

[543]*Id.* Under Article 8 of the Constitution of the Republic of Slovenia, once the Convention is ratified by the Parliament all international legal acts are applicable directly - no futher legislative action implementing the Convention is needed. *See* The Constitution of the Republic of Slovenia, Article 8, http://www.us-rs.si/en/basisfr.html. This means that once the Convention on Cybercrime has been ratified, Slovenia is directly bound by its provisions; in the case of discrepancy between Slovenian law and the Convention, the Convention should prevail. Email from Klemen Tièar to Kimberly Bruce (May 27, 2002) (on file with the authors).

[544]*See* Penal Code of the Republic of Slovenia (December 2000), http://www.oecd.org/pdf/M00024000/M00024167.pdf.

[545]Email from Klemen Tièar to Kimberly Bruce (May 27, 2002) (on file with the authors).

[546]*Id.*

[547] http://www.gov.yu/informatics/index.html

[548] *See* CANADIAN CRIMINAL CODE § 430, http://www.mcconnellinternational.com/services/country/canada.pdf :

> (1) Every one commits mischief who willfully (a) destroys or damages property; (b) renders property dangerous, useless, inoperative or ineffective; (c) obstructs, interrupts or interferes with the lawful use, enjoyment or operation of property; or (d) obstructs, interrupts or interferes with any person in the lawful use, enjoyment or operation of property.
> (1.1)Every one commits mischief who willfully (a) destroys or alters data; (b) renders data meaningless, useless or ineffective; (c) obstructs, interrupts or interferes with the lawful use of data; or (d) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto. . . .
> (5) Every one who commits mischief in relation to data (a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years; or (b) is guilty of an offence punishable on summary conviction.

United States of America

Cybercrime legislation has been adopted at both the state and federal levels. The survey below concentrates on federal legislation, both because of its more general applicability and because the idiosyncrasies of the legislation adopted by the fifty states is quite outside the ambitions of this endeavor.[553]

Federal legislation:

Computer intrusions and other computer-related crimes: Section 1030 of Title 18 of the U.S. Code defines a number of computer-related offenses, e.g., hacking, cracking, virus dissemination, fraud, password trafficking, extortion and fraud. The statute reaches conduct targeting a federal or "protected computer." A "protected computer" is (a) a computer that is used exclusively by a financial institution or the federal government or that is used, albeit nonexclusively, by a financial institution or the federal government and the conduct constituting the offense affects that use; or (b) a computer that is used in interstate or foreign commerce or communication.[554] The statute reaches conduct that inflicts damage to

---

> (5.1) Every one who wilfully does an act or willfully omits to do an act that it is his duty to do, if that act or omission is likely to constitute mischief causing actual danger to life, or to constitute mischief in relation to property or data,
> (a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years; or (b) is guilty of an offence punishable on summary conviction.

[549] *See id*. § 322.

[550] *See id*. § 184.

[551] *See id*. § 380.

[552] *See id*. § 342.1(1):

> (1) Every one who, fraudulently and without (a) obtains, directly or indirectly, any computer service, (b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system, (c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system, or (d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

[553] For a collection and classification of cybercrime laws adopted by the states, *see* Shell Draft: Model State Computer Crimes Code, *available at* http://www.cybercrimes.net/ShellDraft/MSCCCShellDraft.html. *See also* Susan W. Brenner, *State Cybercrime Legislation in the United States of America: A Survey*, 7 RICH. J. L. & TECH. 28 (2001), *at* http://www.richmond.edu/jolt/v7i3/article2.html.

[554] *See* 18 U.S.C. § 1030(e)(2).

individuals or to artificial entities. [555] As to substantive offenses, § 1030(a) makes it a federal crime to do any of the following:

a. To (i) knowingly access a computer without authorization or by exceeding authorized access and thereby obtain information that is protected against disclosure which the perpetrator has reason to believe could be used to the disadvantage of the U.S. or to the advantage of any foreign nation and (ii) willfully either deliver that information to a person not entitled to receive it or retain the information and refuse to deliver it to the federal agent entitled to receive it;

b. To intentionally access a computer without authorization or by exceeding authorized access and thereby obtain (i) information contained in a financial record of a financial institution, or of a card issuer or contained in a file of a consumer reporting agency on a consumer, (ii) information from any federal department or agency, or (iii) information from any protected computer if the conduct involved an interstate or foreign communication;

c. To intentionally and without authorization access (i) a computer used exclusively by a federal department or agency or (ii) a computer not used exclusively by a federal department or agency when the conduct affects the computer's use by or for the federal government;

d. To knowingly and with the intent to defraud access a protected computer without authorization or by exceeding authorized access and thereby further the intended fraud and obtain anything of value unless the object of the fraud and the thing obtained consist only of the use of the computer and the value of that use does not exceed $5,000 in any one-year period;[556]

e. To (i) knowingly cause the transmission or a program, information, code or command and thereby intentionally cause damage to a protected computer; (ii) intentionally access a protected computer without authorization and thereby recklessly cause damage; or (iii) intentionally access a protected computer without authorization and thereby cause damage;

f. To knowingly and with intent to defraud traffic in any password or other information used to access a computer if (i) the trafficking affects interstate or foreign commerce or (ii) the computer to which access can be gained is by or for the federal government;

g. To transmit in interstate or foreign commerce any threat to cause damage to a protected computer with the intent to extort money or any thing of value from any person, firm, association, educational institution, financial institution, government or other legal entity.

Unauthorized access to stored electronic communications: Section 2701(a) of Title 18 of the U.S. Code makes it an offense either (a) to intentionally access without authorization a facility through which an electronic communication is provided or (b) to intentionally exceed an authorization to access such a facility and thereby obtain, alter or prevent authorized access to a wire or electronic communication while it is in electronic storage. The basic punishment is a fine, imprisonment for not more than six months, but the penalties increase if the offense was committed for purposes of commercial advantage, malicious

[555] *See, e.g.,* U.S. v. Middleton, 231 F.3d 1207, 1210-1213 (9th Cir. 2000) (though the statute prohibits conduct causing damage to "one or more individuals", court found that it also reaches conduct which inflicts damage on corporate or other artificial entities).

[556] *See, e.g.,* U.S. v. Bae, 2001 WL 557903 (D.C. 2001); U.S. v. Sadolsky, 234 F.3d 938 (6th Cir. 2000).

destruction or damage or private commercial gain.[557] If the offense is committed for the purpose of commercial advantage, malicious destruction or damage or private commercial gain, the allowable period of imprisonment rises to not more than one year for a first offense and to not more than two years for a subsequent offense.[558]

Sending obscene/offensive material to minors or sending harassing messages: Section 223(a) of Title 47 of the U.S. Code makes it an offense to use a telecommunications device in interstate or foreign communications to: (1) make, create solicit and initiate the transmission of "any comment, request, suggestion, proposal, image, or other communication which is obscene, lewd, lascivious, filthy, or indecent, with intent to annoy, abuse, threaten, or harass another person"; (2) make, create solicit and initiate the transmission of "any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age, regardless of whether the maker of such communication placed the call or initiated the communication"; (3) make a telephone call or "utilize a telecommunications device, whether or not conversation or communication ensues, without disclosing his identity and with intent to annoy, abuse, threaten, or harass any person at the called number or who receives the communications"; (4) make or cause "the telephone of another repeatedly or continuously to ring, with intent to harass any person at the called number"; (5) make repeated telephone calls or repeatedly initiate communication "with a telecommunications device, during which conversation or communication ensues, solely to harass any person at the called number or who receives the communication"; or (6) knowingly permit any telecommunications facility under his or her control to be used to commit any of the previously-listed activities. The penalties for these offenses include fines, imprisonment for up to two years, or both.

Section 223(b) of Title 47 of the U.S. Code makes it an offense: (a) for any person knowingly to use a telephone to make an obscene or indecent communication for commercial purposes or to allow a telephone facility under his or her control to be used for this purpose, or (b) for any person knowingly to use a telephone to make an indecent communication for commercial purposes which is available to anyone under the age or eighteen or to allow a telephone facility under his or her control to be used for this purpose.

The Supreme Court invalidated portions of this statute relating to "indecent" communication by means of a telecommunication device and "patently offensive" communications through use of interactive computer service to persons under the age of 18 on First Amendment grounds in *Reno v. ACLU,* 521 U.S. 844 (1997).

Child Online Protection Act (COPA): Section 231(a)(1) of Title 47 of the U.S. Code makes it an offense to "knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, make[] any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors." It is an affirmative defense that the defendant in good faith restricted minors' access to material that is harmful to them by requiring the use of a credit card or other method of indicating age or by employing "any other reasonable measures that are feasible under available technology."[559] In *ACLU v. Reno*, 217 F.3d 162 (3d Cir. 2000), the Third

[557] *See* 18 U.S. Code § 2701(b).

[558] *See id*.

[559] 47 U.S.C. § 231(c)(1).

Circuit upheld the issuance of an injunction barring enforcement of the statute; the Supreme Court has granted certiorari to review the decision.[560]

Transmitting information about a minor: Section 2425 of Title 18 of the U.S. Code makes it an offense knowingly to initiate "the transmission of the name, address, telephone number, social security number, or electronic mail address of another individual," knowing that person has not attained the age of sixteen, "with the intent to entice, encourage, offer, or solicit any person to engage in sexual activity for which any person can be charged with a criminal offense". The statute also makes it a crime to attempt to violate its provisions.[561]

Fraud in connection with access devices: Section 1029 of Title 18 of the U.S. Code makes it an offense to engage in certain activities involving "access devices," which it defines as "any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used . . . to obtain money, goods, services, or any other thing of value". The statute also prohibits activities involving counterfeit access devices, which it defines as "any access device that is counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device."

Section 1029 makes it an offense to do any of the following: (a) knowingly and with the intent to defraud produce, use or traffic in a counterfeit access device; (b) knowingly and with the intent to defraud traffic in or use one or more access devices during any one-year period and thereby obtain anything of a value aggregating $1,000 or more; (c) knowingly and with the intent to defraud possess fifteen or more devices which are counterfeit or unauthorized access devices; (d) knowingly and with the intent to defraud produce, traffic in, have custody or control of or possess access device-making equipment; (e) knowingly and with the intent to defraud effect transactions with one or more access devices issued to another person or other persons to receive anything of value during any one-year period of a value aggregating $1,000 or more; (f) without the authorization of the issuer of an access device, knowingly and with the intent to defraud solicit someone for the purpose, either, of offering an access device selling information regarding or an application to obtain an access device; (g) knowingly and with the intent to defraud use, produce, traffic in, have custody or control of or possess hardware or software knowing it has been configured to insert or modify telecommunications identifying information associated with or contained in a telecommunications instrument so that the instrument can be used to obtain telecommunications service without authorization; or (h) without the authorization of a credit card owner or its agent, knowingly and with the intent to defraud cause or arrange for another person to present one or more records of transactions made by an access device to the owner or its agent for payment.

State legislation:

Hacking/cracking: Most states make it a crime to purposely access a computer, computer system or network without authorization.[562] Most make it a more serious crime to purposely access a computer without authorization and alter, damage or disrupt the operation of the computer and/or the data it

[560] *See* Ashcroft v. American Civil Liberties Union, ___ U.S. ___, 121 S.Ct. 1997 (2001).

[561] *See* 18 U.S.C. § 2425.

[562] *See, e.g.,* Ind. Code Ann. § 35-43-2-3.

contains.[563] Some states have a "misuse of computer information" statute which prohibits copying, receiving or using information that was obtained by violating a hacking or cracking statute.[564] New York has what is in effect a cyber-burglary statute that makes it a crime to break into a computer or computer system "with an intent to commit or attempt to commit or further the commission of any felony".[565]

Viruses and other harmful programs: A few states outlaw the creation and transmission of virii and other harmful programs,[566] and bills to this effect have been introduced elsewhere.[567]

Miscellaneous computer offenses: A few states make it a crime to introduce false information into a computer system for the purpose of "damaging or enhancing" someone's credit rating.[568] A surprising number have an "offense against computer equipment or supplies," which consists of modifying or destroying "equipment or supplies that are used or intended to be used in a computer, computer system, or computer network".[569] Even more make it a crime to deny, disrupt, degrade, interrupt or cause the denial, disruption, degradation or interruption of computer services or of access to a computer.[570] A few make it a crime to destroy computer equipment.[571] Several states outlaw "computer invasion of privacy," which consists of using a "computer or computer network with the intention of examining any employment, medical, salary, credit, or any other financial or personal data relating to any other person with knowledge that such examination is without authority".[572] Others make it a crime to disclose someone else's computer password.[573]

---

[563] *See, e.g.,* Alaska Stat. § 11.46.740 (Michie 2001); Ark. Code Ann. § 5-41-104 (Michie 2001); Kan. Stat. Ann. § 21-3755 (2001); Neb. Rev. Stat. §§ 28-1345 – 28-1347 (2001).

[564] *See, e.g.,* Ala. Code § 13A-8-102; Conn. Gen. Stat. Ann. § 53a-251; 11 Del. Code Ann. § 935; Florida Stat. § 815.04; Ky. Rev. Stat. Ann. § 434.855; N.H. Stat. Ann. § 638:17.

[565] *See* N.Y. Penal Law § 156.10.

[566] *See, e.g.,* Cal. Penal Code § 502; 720 Ill. Comp. Stat. 5/16D-3; Iowa Code § 716A.3; 17-A Maine Rev. Stat. § 433.

[567] *See, e.g.,* 1999 California Assembly Bill No. 451, California 1999-00 Regular Session; 1999 Pennsylvania Senate Bill No. 1077, Pennsylvania 183rd General Assembly.

[568] *See, e.g.,* Alaska Statutes § 11.46.740; Haw. Rev. Stat. § 708-891; Nev. Rev. Stat. § 205.477; N. M. Stat. § 30-45-4.

[569] *See, e.g.,* Ala. Code § 13A-8-103; Conn. Gen. Stat. Ann. § 53a-251.

[570] *See, e.g.,* Conn. Gen. Stat. Ann. § 53a-251; 11 Del. Code Ann. § 934; Florida Stat. § 815.06; La. Rev. Stat. § 14:73.4; Miss. Code § 97-45-5; WY. Stat. Ann. § 6-3-504.

[571] *See, e.g.,* Conn. Gen. Stat. Ann. § 53a-251; N. H. Stat. Ann. § 638:17; N. J. Stat. Ann. § 2A:38A-3; W. Va. Code § 61-3C-7.

[572] *See* Georgia Code § 16-9-93; 17-A Me. Revised Stat. Ann. § 432; Va. Code Ann. § 18.2-152.5; W. Va. Code § 61-3C-12. *See also* Nev. Rev. Stat. § 205.477 (crime to obtain personal information about another).

[573] *See, e.g.,* Georgia Code § 16-9-93.

Offenses targeting children: A number of states make it a crime to use a computer to solicit or lure a minor to engage in an "unlawful sex act."[574] Several states make it a crime to use a computer to compile information about a child "for the purpose of facilitating, encouraging, offering or soliciting a prohibited sexual act" from that child.[575] These statutes are part of an effort to outlaw child pornography.[576] Many states prohibit using a computer to create, store and/or distribute child pornography,[577] and many also prohibit using a computer to send obscene material to a child.[578] Pennsylvania makes it an offense to use a computer to communicate with a child for the purpose of engaging in prostitution.[579]

Stalking and harassment: Only about sixteen states outlaw online stalking or harassment, and several of them require that an offender transmit a "credible threat" to injure the victim, the victim's family or "any other person."[580] Other statutes are broader, making it a crime to use a computer to "engage in a course of conduct" that would cause a "reasonable person" to "suffer intimidation or serious inconvenience, annoyance or alarm," as well as fearing death or injury to themselves or to members of their family.[581] Some states have expanded their "obscene phone call" statutes so they encompass using the telephone or an "electronic communication device" to contact someone and threaten to injure that person or his/her family, to use obscene language or to make repeated contacts in an effort to annoy the person.[582] A New York court has held that a similar provision encompasses harassing or threatening messages sent via the Internet.[583] Bills have been introduced to make online stalking and/or harassment an offense in states where it is not currently outlawed.[584]

Fraud and theft crimes: A substantial number of states outlaw using computers to commit fraud,[585] i.e., using a "computer, computer system, computer network, or any part thereof for the purpose of devising or

---

[574] *See, e.g.,* Ala. Code § 13A-6-110; Cal. Penal Code § 288.2.

[575] *See, e.g.,* 11 Delaware Code Ann. § 1112A; 21 Okla. Stat. Ann. § 1040.13a; Va. Code § 18.2-374.3.

[576] *See, e.g.,* Fla. Stat. Ann. § 847.0135; Va. Code § 18.2-374.3.

[577] *See, e.g.,* Cal. Penal Code § 311.11; Vernon's Texas Code Ann. § 43.26; Va. Code § 18.2-374.3; Wyo. Stat. § 6-4-303.

[578] *See, e.g.,* Ala. Code § 13A-6-111; Georgia Code § 16-12-100.1.

[579] *See* 18 Penn. Cons. Stat. Ann. § 6318.

[580] *See* Alabama Code § 13A-11-8; West's Rev. Washington Code Ann. § 9A.46.110; Wisconsin Stat. Ann. § 947.0125; WY. Stat. § 6-2-506. *See also* Cal. Penal Code § 422 (offense to transmit "credible threat" even absent intent to carry out threat).

[581] *See* Alabama Code § 13A-11-8; Arizona Rev. Stat. Ann. § 13-2921; West's Rev. Washington Code Ann. § 9A.46.110; Wisconsin Stat. Ann. § 947.0125; WY. Stat. § 6-2-506. *See also* Mass. Gen. Laws 265 § 43.

[582] *See* Ark. Code § 5-41-108; Cal. Penal Code § 653m; Ind. Code Ann. § 35-45-2-2; Kansas Stat. Ann. § 21-4113.

[583] *See* People v. Munn, 179 Misc.2d 903, 688 N.Y.S.2d 384, 385 (N.Y.City Crim.Ct. Feb 09, 1999).

[584] *See, e.g.,* 1999 New Hampshire House Bill No. 345; 1998 New Jersey Assembly Bill No. 3506, New Jersey 208th Legislature.

[585] *See, e.g.,* N. M. Stat. § 30-45-3; N. C. General Stat. § 14-454; N. D. Century Code § 12.1-06.1-08; 21 Okla. Stat. § 1953.

executing any scheme or artifice to defraud" or for "obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises".[586] States tend to incorporate embezzlement crimes into their computer fraud statutes, rather than creating separate "computer embezzlement" provisions.[587] A substantial number of states also outlaw "computer theft,"[588] which can encompass any of several discrete offenses: information theft;[589] software theft;[590] computer hardware theft;[591] and theft of computer services.[592] It can also encompass using a computer to commit a theft in a more traditional sense, e.g., to steal property other than data or computer hardware or software.[593] A few states prohibit the unlawful possession of computer data and/or computer software.[594] Some have "identity theft" statutes, which make it a crime to "knowingly and with intent to defraud for economic benefit" obtain, possess, transfer, use or attempt "to obtain, possess, transfer or use, one or more identification documents or personal identification number of another /person other than that issued lawfully for the use of the possessor."[595]

A few states outlaw computer forgery, which is defined as follows: "Any person who creates, alters, or deletes any data contained in any computer or computer network, who, if such person had created, altered, or deleted a tangible document or instrument would have committed forgery . . . shall be guilty of the crime of computer forgery."[596] At least one state makes it a crime to possess "forgery devices," which include computers, computer equipment and computer software "specifically designed or adapted to such use".[597]

Crimes against government: Only a few states have make it a crime to use computers to obstruct law enforcement or the provision of government services. Illinois forbid using a computer to cause a "disruption of or interference with vital services or operations of State or local government or a public utility".[598] Several states make it a crime to use a computer to interrupt or impair the delivery of essential

[586] *See* Col. Rev. Stat. § 18-5.5-102.

[587] *See, e.g.,* Haw. Rev. Stat. § 708-89; N. M. Stat. § 30-45-3.

[588] *See, e.g.,* Col. Rev. Stat. § 18-5.5-102; Georgia Code § 16-9-93; Haw. Rev. Stat. § 708-891.

[589] *See, e.g.,* Col. Rev. Stat. § 18-4-412; Iowa Code § 716A.9; Minn. Stat. Ann. § 609.89; N. J. Stat. § 2C: 20-25; R. I. General Laws § 11-52-4.

[590] *See, e.g.,* Minn. Stat. Ann. § 609.89; N. J. Stat. § 2C: 20-25 & 2C: 20-33; R. I. General Laws § 11-52-4.

[591] *See, e.g.,* N. J. Stat. § 2C: 20-25; R. I. General Laws § 11-52-4.

[592] *See, e.g.,* Conn. General Stat. § 53a-251; 11 Del. Code § 933; Iowa Code Ann. § 716A.9; Mass. Gen. Laws Ann. 266 § 33A; N.H. Stat. Ann. § 638:17; Va. Code § 18.2-152.6.

[593] *See, e.g.,* La. Rev. Stat. § 14:73.2; Mich. Comp. Laws § 752.795.

[594] *See, e.g.,* W. Va. Code § 61-3C-6.

[595] *See, e.g.,* Ark. Code Ann. § 5-37-227; Georgia Code § 16-9-121.

[596] Georgia Code § 16-9-121. *See also* Nev. Rev. Stat. § 205.481; Va. Code § 18.2-152.14; W. Va. Code § 61-3C-15.

[597] N.J. Stat. Ann. §2C:21-.1.

[598] 720 Ill. Comp. Stat. 5/16D-4.

services (e.g., services of a public or private utility, medical services, communication services or government services) or to otherwise endanger public safety.[599] Some states make it a crime to use a computer to obtain information "with the state or any political subdivision which is by statute required to be kept confidential".[600] West Virginia prohibits the unauthorized accessing of information stored in a computer owned by its state legislature.[601] Rhode Island makes it a crime to use a computer to destroy evidence for the purpose of obstructing an official investigation.[602]

Internet gambling: On June 4, 2001, Nevada legislators approved a bill that would make Nevada the first state to offer legalized Internet gambling.[603] On June 14, 2001, Nevada's governor signed the bill,[604] thereby setting up what may be an interesting legal challenge, since some contend that online gambling, even if legal under Nevada law, would violate federal law.[605]

IV. SOUTH AND CENTRAL AMERICA AND THE CARRIBBEAN

Argentina

In responding to a 1999 survey administered by the Permanent Council of the Organization of American States' Government Experts on Cyber Crime,[606] Argentina indicated that its law did not then

---

[599] *See* W. Va. Code § 61-3C-14; Nev. Rev. Stat. § 205.4765; WY. Stat. Ann. § 6-3-501.

[600] Neb. Rev. Stat. § 28-1346; W. Va. Code § 61-3C-11.

[601] *See* W. Va. Code § 61-3C-4.

[602] *See* R. I. General Laws § 11-52-8.

[603] *See* Nevada Assembly Bill No. 466, http://www.leg.state.nv.us/71st/bills/AB/AB466_EN.html. *See also Nevada Lawmakers OK Internet Betting*, Deseret News (June 5, 2001).

[604] *See, e.g., Just Double Click on YouLose.com; Nevada Bill Paves Way for Online Gambling*, THE ARIZONA REPUBLIC, June 16, 2001, at B6.

[605] *See, e.g.,* Dave Berns, *Internet Gaming in Nevada on Road to Lucrative Reality*, Las Vegas Review Journal (June 7, 2001). *See also* 18 U.S. Code § 1084 (unlawful to use a "wire communication facility" to transmit bets or wagering information in interstate or foreign commerce).

[606] *See* Permanent Council of the Organization of American States, Final Report on the Meetings of Government Experts on Cyber Crime (Preliminary Version), Oct. 28, 1999, http://www.oas.org/juridico/english/Present/finalrep.doc:

> In March 1999 the Ministers of Justice or of Ministers or Attorneys General of the Americas recommended the establishment of an intergovernmental experts group on cyber crime with a mandate to (1) complete a diagnosis of crime targeting computers and information in the member states; (2) complete a diagnosis of national legislation, policies, and practices responsive to such crime; (3) identify national and international entities with relevant expertise; and (4) identify mechanisms of cooperation within the inter-American system to combat cyber crime.

The Committee of Experts was created and held two meetings, in addition to administering the survey discussed in the text, above. *See id.*

penalize "the unauthorized destruction, modification, alteration, access, usage or other similar interference to or of a computer system or program".[607] Asked if its law penalized the "unauthorized erasure, alteration, rendering inaccessible, acquisition, or other similar interference to or of information or data from a computer system or program", Argentina replied that it did to some extent, since "[I]n the area of criminal tax law, Criminal Tax Act No. 24,769, article 12, addresses the fraudulent alteration of records."[608] The questionnaire also asked countries if their law criminalized the "unauthorized interception of the transmission in any manner or mode of computer data or information".[609] Argentina's response was that its law did not specifically outlaw this but that "Article 197 of the [Argentine] Penal Code punishes the interception of telephone communications. Therefore, if data is transmitted via telephone, unauthorized interception could be considered criminal."[610] However, there appears to be a loophole in the Argentinean law, which allows the defacing of webpages because they are not considered material objects.[611]

Barbados

Barbados has not enacted any specific cyber crime legislation.[612]

Brazil

On July 14, 2000, amendments to Brazil's Penal Code were enacted, to go into effect ninety days after the date the amendments were published.[613] The amendments created two new offenses: the "entry of false data" into an information system;[614] and the unauthorized modification or alteration "of the information system or computer program by an employee".[615]

---

[607] Permanent Council of the Organization of American States, Responses Received to the Questionnaire Prepared at the First Meeting of the Government Experts on Cyber Crime, Oct. 5, 1999, 15, http://www.oas.org/juridico/english/Respocyber.doc.

[608] *Id.* at 18.

[609] *Id.* at 20.

[610] *Id.*

[611] http://www. Wired.com/news/print/0,1294,51860,00.html.

[612] Director of Public Prosecutions of Barbados.

[613] *See* Brazil, Law No. 9,983 of July 14, 2000, http://www.mcconnellinternational.com/services/country/brazil.pdf.

[614] *See id*. Article 313-A:

> Entry, or facilitation on the part of an authorized employee of the entry, of false data, improper alteration or exclusion of correct data with respect to the computer system or the data bank of the public administration for purposes of achieving an improper advantage for himself or for some other person, or of causing damages.
>
> Penalty - imprisonment for 2 (two) to 12 (twelve) years, and fine.

[615] *See id*.

Brazil also has a number of cybercrime laws that predate these amendments. Its criminal law defines computer data as "information stored by means of electronic, video or voice equipment, whereas a data base is a collection of information stored by means of electronic, video or voice equipment, which permits the search of said data by manual or electronic procedures of any kind".[616] And Brazilian law defines a computer program as an organized series of instructions in natural or codified language contained on a physical medium of any kind, which requires the use of electronic data processing machinery, devices, instruments or ancillary equipment, based on digital or analog technology, to operate it for certain purposes.[617] The gaining of unauthorized access to a computer system or a violation of the secrecy of a computer system, belonging to either a financial institution or securities dealer is a crime under Article 18 of Law No. 7492, dated June 16, 1986, which defines crimes against the national financial system.

Computer trespass is covered by several Brazilian laws: The violation of data by means of clandestine or hidden access to a computer program or system is also a crime, punishable by imprisonment of six months to one year as is violation of the secrecy of data by gaining access to information contained in the system or physical medium of a third party.[618] If such access results in undue economic benefit to the detriment of the principal of the system, such an act is penalized as stellionate, which is described in Art. 2 of that Law.[619]

Obtaining undue access to a computer system or to an integrated computer network is a crime punishable by a prison term of three to six months, or a fine.[620] If access is gained through wrongful use of the password or code or magnetic identificatino procedure of a third party, the crime is punishable by imprisonment from one to two years and a fine.[621] If, in addition, it results in economic damages to the principal, it is punished with imprisonment of one to three years and a fine.[622] If the purpose of the access is to cause damage to another or to obtain an undue advantage or benefit, the crime is punishable by imprisonment of two to four years and a fine.[623] Further, if the integrated computer network or system belongs to a public corporate entity under Brazilian law, or to a decentralized agency, public enterprise, semi-public company, or foundation instituted or maintained by the national government, or independent social services, the punishment is enhanced by one-third.[624]

---

[616]Art. 2, i. of Bill PL 0173 1996 in the Chamber of Deputies.

[617] Art. 1 of Law No. 9609 of February 19, 1998.

[618]PLS 00152, Art. 1 ¶ 1 (1991) (Senate bill that defines crimes involving wrongful use of computers and contains other provisions).

[619]*Id.* at Art. 1 ¶ 1(b).

[620] *Id.* at Art. 18.

[621]*Id.* at Art. 18 ¶ 1.

[622]*Id.* at Art. 18 ¶ 2.

[623]*Id.* at Art. 18 ¶ 3.

[624]*Id.* at Art. 18 ¶ 4.

Brazil has several laws prohibiting the interception of telephone, data, or telematic communications. These laws ensuring privacy and criminalizing data interception are outlined in both the Brazilian Federal Constitution as well as in public law.[625]

On August 8, 2001, "Project de Lei da Camara n. 84/1999," a bill specifically targeted at cybercrimes, was submitted to the House of Representatives.[626] If the House passes the bill it will be sent to the President for his approval.[627]

Chile

Chile's Law on Automated Data Processing Crimes no. 19.223, published June 7, 1993 criminalizes espionage on automated systems. [628]

---

[625]This is a summary of those provisions:

- The privacy, intimate life, honor, and reputation of persons are inviolable, and the law provides for compensation for moral prejudice and physical damages when they are violated. (Federal Constitution, Art. 5, X).
- The confidentiality of correspondence, telegraph or cable communications, data, and telephone communications is inviolable, with the exception, in the latter case, of a judicial order, in the circumstances and in the manner established by law for the purposes of a criminal investigation or of gathering evidence for a preliminary [pretrial] criminal hearing [*instrucao processual penal*] (*Id.* at Art. 5, XII).
- It is a crime to intercept telephone, computer, or telematic communications, or to violate court secrecy, without judicial authorization or for unauthorized purposes. This crime is penalized by imprisonment from two to four years and a fine (Article 10 of Law No. 9296 of July 24, 1996, regulating the final part of section XII, Article 5, of the Federal Constitution).
- *Habeas data* is granted in the following cases: to ensure knowledge of the information regarding the petitioner appearing in records or in data banks of government or public institutions (Federal Constitution, Art. 5, LXXII, "a");
- Law No. 9507 of November 12, 1997 regulates the right of access to information and the procedures involved in *habeas data*.
- Articles 43 and 44 of Law No. 8078 of September 11, 1990, which contains provisions on consumer protection, among others, regulates or controls data banks and consumer records.
- and, for correction of data, when the preference is not to do so by a confidential, judicial, or administrative procedure (idem, Art. 5, LXXII, b.).

[626]Information provided by Vladimir Aras, Promotor de Justica, BA, Brazil; Professor de Processo Penal e de Direito Internacional Publico na UEFS.

[627] *Id.*

[628] Schjolberg, *supra* note 164. *See* McConnell International, *Cyber Security Legislation - Chile*, http://www.mcconnellinternational.com/services/Updatedlaws.htm:

Costa Rica

Costa Rican law does not currently have specific laws that prohibit computer trespass, tampering with a computer system, or computer related theft. These crimes, when possible, would be prosecuted other under general criminal statues such as theft.

The Costa Rican Penal Code however is currently undergoing substantial revision. The Costa Rican Attorney General has indicated that "it would be advisable to introduce categories that specifically protect legal interests related to computers, so that the special nature of the matter can be taken into account when the punishment is established."

The proposed comprehensive Penal Code reform (Draft law No. 11,871) provides protection for a number of legal interests tied to "cybercrimes," but does not do so in a special way or cover the subject in a separate section. Instead, this is included in defined crimes against privacy (Title IV: Offenses Related to the Violation of Privacy) in Chapter I, the heading of which is[629] "Tampering with Personal Data and Communications."

> Article 1 - The one that maliciously destroys or makes unusable a system of information processing or its parts or components, or prevents or modifies its operation, will be undergo the punishment of prison from average to maximum degree. If, as a result of this action, the data contained in the system will be
> affected, the punishment indicated in the previous interjection will be applied in its maximum degree.
>
> Article 2 - The one that attempts illegally to seize, to use, or to know the information contained in an information processing system or to intercept or interfere or have access to it, will be punished with a minor to medium jail sentence.
>
> Article 3 - The one that maliciously alters, damages or destroys the data contained in a system of information processing, will be punished with a prison sentence of minor to a medium degree.
>
> Article 4 - The one that maliciously reveals or spreads the data contained in an IS will undergo the punishment with a prison sentence of minor to medium sentence. If the person who incurs these conducts is the person in charge of the IS, the punishment will be increased in degree.

[629] The following offenses are covered in the draft legislation:

> Article 185. Illegal handling of personal data and communications.
>
> A penalty of one to four years in prison shall be imposed on anyone who illegally obtains information about, takes possession of, copies, transmits, publishes, compiles, uses, intercepts, retains, opens, suppresses, conceals, diverts, or otherwise engages in the unauthorized handling of communications, images, or data, neither public nor well-known, belonging to another person, without the express consent of the person affected.
>
> A penalty of six months to two years in prison shall be imposed on anyone who, being in legal possession of communications, images, or data that are not intended to be publicized, publicizes them without due authorization, even though they may have been sent to him.
>
> The same penalty shall be imposed on anyone who, either by commission or by omission, facilitates the commission of any of the acts described above by another person.

Cuba

A study published in December of 2000 found that while Cuba currently had no cybercrime specific laws in place, a working group from the Ministry of Justice was drafting cybercrime legislation.[630] In looking at the need for new legislation addressing cybercrimes, the working group found that "a great number of them" are covered by Cuba's present Penal Code, but still developed some modifications that might improve the Penal Code's ability to address cybercrimes.[631] One such modification would make the use of a computer to commit a crime an aggravating factor, just as the use of a firearm is an aggravating factor under the laws of many countries.[632] The working group also drafted possible revisions of three existing offenses[633] and sections defining new crimes.[634]

> Article 186. Obtaining personal data by deceptive means
>
> A penalty of one to three years in prison shall be imposed on anyone who, by engaging in trickery or deception, obtains personal information, neither public nor well-known, belonging to another person.
>
> Article 187. Violation of the security and confidentiality of personal data
>
> A penalty of six months to two years in prison shall be imposed on anyone who has under his control, or in his custody or possession, personal information, neither public nor well-known, and fails to take the necessary security measures to protect its confidential, restricted, or secret nature.
>
> A penalty of one to four years in prison shall be imposed on anyone who violates the security measures mentioned in the foregoing paragraph for the illegal purpose of obtaining information about, copying, transmitting, publishing, compiling, using, or handling in an unauthorized manner personal information, neither public nor well-known, which is held by someone other than the person to whom that information belongs.
>
> The penalty indicated in the foregoing paragraph also shall be imposed on anyone who, having knowledge of information the confidentiality of which he is legally bound to maintain, discloses it without just cause in a way that may cause harm.
>
> The same penalty shall be imposed on anyone who uses, disseminates, or discloses information he knows to have been obtained unlawfully.

[630] *Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information, supra* note 1.

[631] Cuban Ministry of Justice Working Group Report, http://www.mcconnellinternational.com/services/country/cuba.pdf.

[632] *See id.*

[633] *See id.:*

> **Article 334. 1.**
>
> If the culprit, to carry out the fact, uses some computer manipulation or similar artifice that allows him to obtain a not authorized transfer of any patrimonial asset in damage of another person, the sanction is ___ freedom deprivation?
>
> **Article 339 or 340.**

Ecuador

There are no criminal laws in Ecuador which prohibit "computer crimes" such as computer trespass, vandalism, or interception of computer communications. Ecuador's penal code does not speak of cybercrime. Ecuador does however monitor and investigate computer piracy, defined as the use of computers to duplicate computer programs or phonographic works in violation of copyright law. Thus, Ecuadorian law punishes only the alteration or modification of electronic information as regards copyright provisions, under Articles 26 and 324 of the Intellectual Property Act.

The Government of Ecuador could provide no specific data on any particular computer crimes which might have occurred in the country. Statistics on computer crime are not available, since these crimes are in a gray area and hard to trace.

Since there are no laws prohibiting most common forms of computer crime in Ecuador, the government has stated that it has no jurisdiction to investigate and prosecute these matters. The only exception once again is computer piracy, to which the procedure established under Decision 351 of the Andean Community of Nations and the Ecuadorian Intellectual Property Act is applied.

> Who by any means, destroys, alters, disables, or in any other way, he damages the data, programs or other people's electronic documents, included in networks, electronic supports or computer systems, will be sanctioned to _____freedom deprivation or to fine? . . .
>
> **Article 259.1**
>
> Who manufactures or introduce in the country, stamps, presses, marks or other class of means or instruments dedicated well-knownly to the falsification...
> In same sanction it incurs who creates or introduce in the country, computer programs to carry out falsifications mentioned in the previous sections or utilizes telematic means to alter information contained in computer supports.

[634] *See id.:*

> Who utilizes any terminal equipment of telecommunication, without consent of its holder, causing him damage of considerable value, will be sanctioned to ____freedom deprivation or to fine?. . .
>
> Who creates, distributes, trades or illegitimately posess harmful computer programs as computer virus, trojans, logical bombs or other similar ones, will be sanctioned ___ freedom deprivation or fine? . . .
>
> Who intentionally, without the due authorization or exceeding it, intercepts, interferes, uses, alters, damages or destroys, a system or computer network, a logical support, a computer program or database, or any other computer application, completely or partly, will be sanctioned to_____freedom deprivation or fine?.
>
> If the fact has for object to obtain an undue benefit for him or for a third, will be sanctioned to _____freedom deprivation or fine?
>
> Who by negligence, allows another not authorized person to access, intercepts, interferes, uses, alters, damages or destroys a system or computer network, a logical support, calculation program or base data, or any other computer application completely or partly, will be sanctioned to ____ freedom deprivation or fine?

Furthermore, in Ecuador, the seizure of intangible computer data is not permitted, because there is no law expressly permitting it. However, for the protection of intellectual property, it is permissible to seize the physical medium used to store programs or data that

El Salvador

The government of El Salvador has no specific **Article 334. 1.**4. If the culprit, to carry out the fact, uses some computer manipulation or similar artifice that allows him to obtain a not authorized transfer of any patrimonial asset in damage of another person, the sanction is ___ freedom deprivation?police or prosecutorial agency which has taken responsibility for the investigation and prosecution of computer crime. Additionally, El Salvador reports that they have had no significant incidents of computer crime within their country.

There are no laws on the books in El Salvador which prohibit the alteration, interception, or destruction of computer information. Computer systems are not defined nor referenced within El Salvadorian criminal law. Despite the lack of substantive law relative to computer crime in El Salvador, training courses on the subject have been started and are in progress in the Office of the Attorney General of the Republic.

Mexico

Article 211(1) to 211(7) of the Mexican Federal Penal Code prohibits the copying, modification, destruction or damaging information, databases, or computers or information systems.[635]

Nicaragua

A study published in December of 2000 found that Nicaragua had no cybercrime specific laws in place. [636]

Panama

In the Republic of Panama there are no specifically defined and punishable crime relating to computer crime. There is, however, the concept of "damage," within the meaning of "crimes against property," in which computers are considered as the property of another.

The Criminal Code of the Republic of Panama does penalize the destruction of a computer system, seen from the perspective that the computer system is another person's property. This is the sense of Article 200 of the Criminal Code, relating to "damage" under the heading "Crimes against property." It is unknown, however, whether any prosecutions have taken place under this theory in Panama to date.

The Criminal Code of the Republic Panama does not specifically penalize the unauthorized destruction, modification, alteration, access, usage, or other similar interference to or of a computer system or program, from the perspective of "cybercrime."

---

[635] *See* Permanent Council of the Organization of American States, *supra* note 602.

[636] *See Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information, supra* note 1.

Peru

In April of 2000, Peru added two computer crime provisions to its Penal Code. The provisions criminalize the unauthorized use of a computer system and damaging, altering or destroying data or computer programs. [637]

Trinidad and Tobago

At this time, there is no specific computer crime legislation, but Trindad and Tobago are in the process of finalizing specific legislation – The Computer Misuse Bill, 1999. This bill provides the following offenses and penalties:

Clause 5 – Unauthorized modification of computer material;
Clause 3 – Unauthorized access to computer material
Clause 6 – Unauthorized use or interception of computer service
Clause 7 – Unauthorized obstruction of use of computer
Clause 8 – Unauthorized disclosure of access code
Clause 10 – Unauthorized receiving or giving access to data.

Venezuela

Venezuelan law does not criminalize the destruction, modification, alteration, or interference to or of a computer system or program. In the case of interference and other harmful activity that targets information and data of computer systems or programs, penalties exist in Venezuela that are applicable to the content of communications. These provisions are expressed in Articles 2 and 4 of the Law on the Protection of the Privacy of Communications, which states:

> Article 2. Anyone who arbitrarily, clandestinely, or fraudulently records or intercepts a communication between two persons, or interrupts it or blocks it, shall receive a prison sentence of three to five years.
>
> Article 4. Anyone who, in order to obtain some benefit for himself or others or in order to produce damage, forges or alters the content of a communication, shall receive a prison sentence of three to five years, provided that he used said content or allowed others to use it.

---

[637] *See* Peru, Legislative Decree No. 635, Chapter XI, Computer Crimes, http://www.mcconnellinternational.com/services/country/peru.pdf:

> **Article 208-A.** Any individual who inappropriately enters or uses a database, computer system or network, or any part thereof, to design, implement, copy or modify a scheme or similar item will be punished by imprisonment not to exceed two years or the provision of between fifty-two and one hundred-four days of community service. If the agent acts with the purpose of defrauding or obtaining an economic benefit (goods or information), he or she will be punished by imprisonment not to exceed three years or the provision of community service in an amount no less than one hundred four days.
>
> **Article 208-B.** Any individual who improperly interferes, uses, modifies, damages or destroys a medium or computer program or information in transit between or contained within the latter or in the base, systems or network, will be punished by imprisonment of no less than three nor more than five years and a fine of between sixty and ninety days.

> The same penalty shall be imposed on anyone who uses or exploits the content of a forged or altered communication, or even though that person did not participate in its falsification or received it from an anonymous source.

Venezuelan criminal law does penalize the unauthorized interception and transmission of computer data and information. Article 2 of the Law on the Protection of the Privacy of Communications published in Official Gazette No. 34,863 of December 16, 1991 states:

> Article 2
>
> Anyone who arbitrarily, clandestinely, or fraudulently records, or obtains information about a communication between two persons, or interrupts it or blocks it, shall receive a prison sentence of three to five years.
>
> Anyone who discloses, in whole or in part, using any means of communication, the content of the communications indicated in the first part of this article shall receive the same penalty, unless the act constitutes a more serious offense.

In that regard, the Organic Draft Law on the General Telecommunications System also establishes administrative sanctions for cases of interference with telecommunications systems, as can be seen in the wording of this law:

> Article 145
>
> A fine of 100 to 1,000 taxation units shall be imposed on anyone who intentionally causes interference that is prejudicial to the operators or users of telecommunications services. If this interference results in the interruption of a legally installed telecommunications service, the fine shall be 500 to 2,000 taxation units.

V. ASIA

Bangladesh

Bangladesh's responses to a United Nations survey on cybercrime law indicate that it has not adopted cybercrime-specific penal legislation.[638]

Burma (Myanmar)

In September 1996, the country enacted the Computer Science Development Law. This legislation includes titles, definitions, and objectives for computer development within Burma (Myanmar). This act also contains a section on prior sanctions and licenses[639], as well as offences and penalties.[640]

---

[638] *See* Kaspersen & Lodder, *supra* note 441.

[639] *See* Union of Myanmar, The State Law and Restoration Council Law No. 10/96, The Computer Science Development Law – Chapter IX ("Prior Sanction and License"), The 8th Waxing of Tawthalin, 1358 M.E. (Sept. 20, 1996), http://www.myanmar.com/gov/laws/computerlaw.html:

1. (a) The Ministry of Communications, Posts and Telegraphs may, with the approval of the Council, determine by notification the types of computer to be imported, kept in possession or utilized only with the prior sanction of the Ministry.
(b) In determining the types of computer under sub-section(a), fax-modem card installed computer which can transmit or receive data shall be primarily targeted.
(c) In determining the types of computer under sub-section(a), it shall not apply to computers that are used only as aids in teaching, office work or business.

2. A person desirous of importing, keeping in possession or utilizing the type of computer prescribed in sub-section (a) of section 26 shall apply to the Ministry of Communications, Posts and Telegraphs in accordance with the stipulations to obtain prior sanction.

3. A person desirous of setting Lip a computer network or connecting a link inside the computer network shall apply to the Ministry of Communications, Posts and Telegraphs in accordance with the stipulations to obtain prior sanction.

4. The Ministry of Communications, Posts and Telegraphs may, after scrutinizing the applications submitted under section 27 or section 28 in accordance with the stipulations, grant prior sanction or refuse to grant prior sanction.

5. A person desirous of keeping in possession or utilizing the type of computer prescribed under sub-section (a) of section 26, shall comply with the orders and directives issued from time to time by the Ministry of Communications, Posts and Telegraphs with respect to issuance of licence, prescribing the term of licence, licence fee and licence conditions

[640] *See id.* at Chapter X ("Offences and Penalties"):

1. Whoever imports or keeps in possession or utilizes any type of computer prescribed under sub-section(a) of section 26, without the prior sanction of the Ministry of Communications, Posts and Telegraphs shall, on conviction be punished with imprisonment for a term which may extend from a minimum of 7 years to a maximum of 15 years and may also be liable to a fine.

2. Whoever sets up a computer network or connects a link inside the computer network, without the prior sanction of the Ministry of Communications, Posts and Telegraphs shall, on conviction be punished with imprisonment for a term which may extend from a minimum of 7 years to a maximum of 15 years and may also be liable to a fine.

3. Whoever fails to comply with a prohibitory order issued by the Council, or the 'Ministry of Education or the Ministry of Communications, Posts and Telegraphs ill respect of the type of computer prescribed under Sub-section(a) of section 26 shall, on conviction be punished with imprisonment for a term which may extend to 6 months or with fine or with both.

4. Whoever commits any of the following acts using computer network or any information technology shall, on conviction be punished with imprisonment for a term which may extend from a minimum of 7 years to a maximum of 15 years, and may also be liable to a fine:-
(a) carrying out any act which undermines State Security, prevalence of law and order and community peace and tranquility, national unity, State economy or national culture;
(b) obtaining or sending and distributing any information of State secret relevant to State security, prevalence of law and order and community peace and tranquility, national unity, State economy or national culture.

5. Whoever violates any order relating to control issued by the Council under Sub-section(c) and Sub-section (d) of section 7 shall, on conviction be punished with imprisonment for a term which may extend to 3 years or with fine or with both.

People's Republic of China

The bulk of China's cybercrime provisions are contained in its "Computer Information Network and Internet Security, Protection and Management Regulations", which were promulgated to "strengthen the security and the protection of computer information networks and of the Internet, and to preserve the social order and social stability."[641] The prohibited activities are set forth in four Articles of the Regulations, to wit:

> **Article 4:** No unit or individual may use the Internet to harm national security, disclose state secrets, harm the interests of the State, of society or of a group, the legal rights of citizens, or to take part in criminal activities.
>
> **Article 5:** No unit or individual may use the Internet to create, replicate, retrieve, or transmit the following kinds of information:
>
> (1) Inciting to resist or breaking the Constitution or laws or the implementation of administrative regulations;
> (2) Inciting to overthrow the government or the socialist system;
> (3) Inciting division of the country, harming national unification;
> (4) Inciting hatred or discrimination among nationalities or harming the unity of the nationalities;
> (5) Making falsehoods or distorting the truth, spreading rumors, destroying the order of society;
> (6) Promoting feudal superstitions, sexually suggestive material, gambling, violence, murder,
> (7) Terrorism or inciting others to criminal activity; openly insulting other people or distorting the truth to slander people;
> (8) Injuring the reputation of state organs;
> (9) Other activities against the Constitution, laws or administrative regulations.

---

6. Whoever imports or exports any type of computer software or any information prescribed by the Council under sub-section (g) of section 7 shall, on conviction be punished with imprisonment for a term which may extend from a minimum of 5 years to a maximum of 10 years and may also be liable to a fine.

7. Whoever fails to comply with an order abolishing any computer association, issued by the Council under sub-section (j) of section 7 shall, on conviction be punished with imprisonment for a term which may extend to 3 years, or with fine or with both.

8. Whoever attempts or conspires to commit any offence under this law or abets in the commission of such offence shall, on conviction be punished with the same penalty prescribed in this Law for such offence.

9. The Court shall, in ordering a penalty for any offence under this Law, confiscate or destroy or dispose of the exhibits relevant to the offence in a accordance with the stipulations.

http://www.myanmar.com/gov/laws/computerlaw.html

[641] People's Republic of China, Computer Information Network and Internet Security, Protection and Management Regulations, Chapter 1 – Article 1, http://a152.g.akamai.net/7/152/1483/79c25fc4e4a63a/www.chinaonline.com/refer/legal/laws_regs/pdf/c00012670e.pdf. *See also id.* at Chapter 1 – Article 1 ("The security, protection and management of all computer information networks within the borders of the PRC fall under these regulations").

> **Article 6:** No unit or individual may engage in the following activities which harm the security of computer information networks:
>
> (1) No one may use computer networks or network resources without getting proper prior approval
> (2) No one may without prior permission may change network functions or to add or delete information
> (3) No one may without prior permission add to, delete, or alter materials stored, processed or being transmitted through the network.
> (4) No one may deliberately create or transmit viruses.
> (5) Other activities, which harm the network, are also prohibited.
>
> **Article 7:** The freedom and privacy of network users is protected by law. No unit or individual may, in violation of these regulations, use the Internet to violate the freedom and privacy of network users.[642]

For violations of Articles 5 and 6, "the Public Security organization gives a warning and if there [is] income from illegal activities, confiscates the illegal earnings."[643] Violations of Articles 4 and 7 are "punished according to the relevant laws and regulations."[644]

Article 287 of the criminal code makes in an offense to "use a computer for financial fraud, theft, corruption, misappropriation of public funds, stealing state secrets or other crimes".[645]

In January of 2000, China implemented "State Secrecy Protection Regulations For Computer Information Systems on the Internet".[646] These Regulations are intended to "to strengthen the management of secrets for the computer systems on the Internet and to ensure the safety of state secrets."[647] They establish a series of procedures which are designed to prevent the advertent or inadvertent disclosure of China's "state secrets,"[648] a term which is "used very loosely and can mean any information not officially approved for publication."[649]

---

[642] *Id.*

[643] *Id.* at Chapter 4 – Article 20.

[644] *Id.* at Chapter 4 – Article 22. As to Article 4, the punishments for "crimes of endangering national security" are set out in Part II, Chapter 1 of the Criminal Law of the People's Republic of China. *See* CHINALAW WEB, http://www.qis.net/chinalaw/lawtran1.htm. As to the punishments that may be available for violating Article 7, *see id.* part II, Chapter 4.

[645] *See, e.g.,* Criminal Law of the People's Republic of China, Article 287, http://www.qis.net/chinalaw/prclaw60.htm#Chapter%20V2.

[646] State Secrecy Protection Regulations For Computer Information Systems on the Internet, CHINA ONLINE, http://www.chinaonline.com/refer/legal/NewsArchive/secure/2000/February/c00012601.asp.

[647] *Id.* at Chapter I – Article 1.

[648] *See id.* at Chapters II & III.

[649] Lester J. Gesteland, *Internet Censored Further in China*, CHINA ONLINE, Jan. 26, 2000, http://www.chinaonline.com/refer/legal/NewsArchive/secure/2000/February/c00012651.asp.

Hong Kong

Telecommunication Ordinance § 27A prohibits unauthorized access to a computer by telecommunication.[650] Section 161 of the Crimes Ordinance covers obtaining access to a computer with criminal or dishonest intent.[651] Section 60 of the Crimes Ordinance, which prohibits damaging or destroying property,[652] encompasses the misuse of a computer, which is defined as follows:

> `misuse of a computer' means-
>
> (a) to cause a computer to function other than as it has been established to function by or on behalf of its owner, notwithstanding that the misuse may not impair the operation of the computer or a program held in the computer or the reliability of data held in the computer;
> (b) to alter or erase any program or data held in a computer or in a computer storage medium;
> (c) to add any program or data to the contents of a computer or of a computer storage medium,
> and any act which contributes towards causing the misuse of a kind referred to in paragraph (a), (b) or (c) shall be regarded as causing it.[653]

Also, burglary, which is defined by § 11 of the Theft Ordinance, [654] encompasses causing damage to a computer as part of its prohibition on entering a building with the intent to commit an offense

---

[650] *See* Hong Kong Ordinances, Chapter 106 -Telecommunication Ordinance, § 27A(1), http://www.justice.gov.hk/home.htm ("Any person who, by telecommunication, knowingly causes a computer to perform any function to obtain unauthorized access to any program or data held in a computer commits an offence and is liable on conviction to a fine of $ 20000").

[651] *See id*. at Chapter 200 - Crimes Ordinance, § 161:

> (1) Any person who obtains access to a computer-
> (a) with intent to commit an offence;
> (b) with a dishonest intent to deceive;
> (c) with a view to dishonest gain for himself or another; or
> (d) with a dishonest intent to cause loss to another,
> whether on the same occasion as he obtains such access or on any future occasion, commits an offence and is liable on conviction upon indictment to imprisonment for 5 years.
> (2) For the purposes of subsection (1) 'gain'and 'loss' are to be construed as extending not only to gain or loss in money or other property, but as extending to any such gain or loss whether temporary or permanent; and-
> (a) 'gain' includes a gain by keeping what one has, as well as gain by getting what one has not; and
> (b) 'loss' includes a loss by not getting what one might get, as well as a loss by parting with what one has.

[652] *See id*. at Chapter 200 - Crimes Ordinance, § 60.

[653] *Id*. at Chapter 200 - Crimes Ordinance, § 59.

[654] *See id*. at Chapter 210 - Theft Ordinance, § 11.

consisting of theft, causing bodily harm or "doing unlawful damage to the building or anything therein."[655]

India

India's cybercrime legislation is set out in "The Information Technology Act, 2000".[656] The offenses are set out in Chapter XI of the Act.[657] They include: tampering with computer source documents;[658] unauthorized access; [659] damaging or destroying computer data; [660] publishing obscenity; [661] disclosing confidential information without authorization; [662] publishing a false digital signature certificate; [663] and creating or publishing a digital signature certificate for fraudulent purposes. [664]

---

[655] *See id*. at Chapter 210 - Theft Ordinance, § 11(1)-(2). *See also id*. at Chapter 210 - Theft Ordinance, § 11(3(A):

> The reference in subsection (2)(c) to doing unlawful damage to anything in a building includes-
> (a) unlawfully causing a computer in the building to function other than as it has been established by or on behalf of its owner to function, notwithstanding that the unlawful action may not impair the operation of the computer or a program held in the computer or the reliability of data held in the computer;
> (b) unlawfully altering or erasing any program, or data, held in a computer in the building or in a computer storage medium in the building; and
> (c) unlawfully adding any program or data to the contents of a computer in the building or a computer storage medium in the building.

[656] Republic of India, The Information Technology Act, 2000, http://www.mit.gov.in/itbillonline/it_framef.htm. *See also* The Electronic Commerce Support Act, 1998, Chapter 2 ("Amendments to the Indian Penal Code"), http://commin.nic.in/doc/ecact2.htm#h2 http://commin.nic.in/doc/ecact2.htm#h2

[657] *See* Republic of India, The Information Technology Act, 2000, http://www.mit.gov.in/itbillonline/it_framef.htm.

[658] *See id.* at Chapter XI - § 65.

[659] *See id.* at Chapter XI - § 70:

> (1) The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system.
>
> (2) The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub-section (1).
>
> (3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

[660] *See id.* at Chapter XI - § 66 ("Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack").

[661] *See id.* at Chapter XI - § 67.

[662] *See id.* at Chapter XI - § 72.

[663] *See id.* at Chapter XI - § 73.

Japan

Japan's cybercrime legislation is contained in two enactments, the "Unauthorized Computer Access Law,"[665] and the "Computer Crime Act."[666] The Unauthorized Computer Access Law creates two offenses: unauthorized computer access[667] and facilitating unauthorized computer access.[668] The Computer Crime Act creates five: computer forgery;[669] disrupting the operations of a business computer;[670] computer theft;[671] computer fraud;[672] and destroying computer records.[673] In April of

---

[664] *See id.* at Chapter XI - § 74.

[665] *See* Japan, Unauthorized Computer Access Law (Law No. 128 of 1999), http://www.npa.go.jp/hightech/fusei_ac2/UCAlaw.html.

[666] Computer Crime Act – Japan Penal Code, http://www.isc.meiji.ac.jp/~sumwel_h/Codes/comp-crim.htm.

[667] *See* Japan, Unauthorized Computer Access Law (Law No. 128 of 1999), Article 3, http://www.npa.go.jp/hightech/fusei_ac2/UCAlaw.html:

> No person shall conduct an act of unauthorized computer access.
>
> . . .The act of unauthorized computer access . . . means . . . :
>
> (1) . . . making available a specific use which is restricted by an access control function by making in operation a specific computer having that access control function through inputting into that specific computer, via telecommunication line, another person's identification code for that access control function . . . ;
> (2) . . . making available a restricted specific use by making in operation a specific computer having that access control function through inputting into it, via telecommunication line, any information (excluding an identification code) or command that can evade the restrictions placed by that access control function on that specific use . . . ;
> (3) . . . making available a restricted specific use by making in operation a specific computer, whose specific use is restricted by an access control function installed into another specific computer which is connected, via a telecommunication line, to that specific computer, through inputting into it . . . any information or command that can evade the restrictions concerned.

[668] *See id*. at Article 4:

> No person shall provide another person's identification code relating to an access control function to a person other than the access administrator for that access control function or the authorized user for that identification code, in indicating that it is the identification code for which specific computer's specific use, or at the request of a person who has such knowledge, excepting the case where such acts are conducted by that access administrator, or with the approval of that access administrator or of that authorized user.

[669] *See* Computer Crime Act – Japan Penal Code, § 161-2, http://www.isc.meiji.ac.jp/~sumwel_h/Codes/comp-crim.htm.

[670] *See id*. § 234-2.

[671] *See id*. § 235 (defining theft) & § 245 (defining electricity as property subject to theft).

2002, Japanese officials announced that they intended to put forward legislation which would criminalize the online transmission of child pornography; while the sale and distribution of child pornography is already illegal in Japan, the law does not outlaw "show[ing] pornographic images of children on . . . websites."[674]

Malaysia

Malaysia's cybercrime legislation is contained in the "Computer Crimes Act 1997."[675] The Act creates four offenses: unauthorized access;[676] unauthorized access with intent to commit or facilitate commission of further offense;[677] unauthorized modification of the contents of a computer;[678] and wrongful communication.[679] It also criminalizes aiding and abetting and attempting to commit any of these offenses.[680]

Mauritius

Mauritius' cybercrime legislation is the product of its "Information Technology Act 1998".[681] Section 4 of the Act amended the Mauritius Criminal Code to add two new offenses: a data protection and security offense;[682] and computer misuse.[683]

---

[672] *See id*. § 246-2 (fraud) & § 250 (attempted fraud).

[673]*See* id. § 258 (destruction of official records) § 259 (destruction of private records).

[674]*See Japan Sets Sights on Online Child Porn,* BBC News (April 19, 2002), http://news.bbc.co.uk/hi/english/sci/tech/newsid_1939000/1939237.stm.

[675] Malaysia, Computer Crimes Act 1997, http://www.ktkm.gov.my/organisation/acts/crimeact.html.

[676] *See id*. at Part II - § 3 ("A person shall be guilty of an offence if he causes a computer to perform any function with intent to secure access to any program or data held in any computer; the access he intends to secure is unauthorised; and he knows at the time when he causes the computer to perform the function that that is the case").

[677] *See id*. at Part II - § 4 (A person shall be guilty of an offence under this section if he commits an offence referred to in commit or facilitate section 3 with intent to commit an offence involving fraud or dishonesty or which causes injury as defined in the Penal Code; or to facilitate the commission of such an offence whether by himself or by any other person").

[678] *See id*. at Part II - § 5 ("A person shall be guilty of an offence if he does any act which he knows will cause unauthorised .modification of the contents of any computer")

[679]*See id*. at Part II - § 6 ("A person shall be guilty of an offence if he communicates directly or indirectly a number, code, password or other means of access to a computer to any person other than a person to whom he is duly authorised to communicate").

[680]*See id*. at Part II - § 7.

[681] Mauritius, Information Technology Act 1998, http://ncb.intnet.mu/ncb/security/itact.htm.

[682]*See id*. § 4:

> **300A. Data protection and security**
>
> (1) [omitted]

Pakistan

Pakistan enacted the PAK Ordinance, which specifically addresses hacking, and virus related offenses.[684] The PAK fails to address obscenity, cyber fraud, intellectual property rights, content

---

(2) [omitted]

(3) Where a data user or computer service person holds or is in possession of personal data which is not accurate, the data user or computer service person, as the case may be, shall commit an offence.

(4) Where a data user or computer service person holding or in possession of personal data -

(a) permits any unauthorised access to, or alteration or disclosure of, the personal data;

(b) holds or possesses the personal data in such a manner that they are likely to be accidentally lost, partially or totally damaged, or destroyed,

the data user or computer service person shall commit an offence.

(5) Any person who commits an offence under subsection (3) or (4) shall, on conviction, be liable to penal servitude for a term not exceeding 10 years and to a fine not exceeding 100,000 rupees.

[683] *See id*. § 4:

369A. Computer misuse

Any person who -

(a) wilfully and in defiance of the rights of another person, impedes or tampers with the operation of a computer;

(b) wilfully and in defiance of the rights of another person, directly or indirectly introduces data into a computer or suppresses or modifies any data which it contained or the method of treatment or transmission of such data;

(c) commits, in a computerised document of whatever form, a forgery of a kind which is likely to cause prejudice to another person;

(d) knowingly makes use of a document referred to in paragraph (c);

(e) without the consent of the person to whom a computer is entrusted, gains access to, or so maintains himself in, the computer,

shall commit an offence and shall, on conviction, be liable to penal servitude for a term not exceeding 10 years and to a fine not exceeding 100,000 rupees.

See also id. § 4:

369B. Aggravating circumstance

A person who commits an offence under section 369 A(e) shall, on conviction, be liable to penal servitude for a term not exceeding 20 years and to a fine not exceeding 200,000 rupees where, as a result of the commission of the offence, data contained in the computer is suppressed or modified or the operation of the computer is altered.

[684] http://www.naavi.org/cl_editorial/edit_17jan_02_3.html.

filtering, censorship and Spamming[685]. Instead, it leaves these offenses to be covered under existing common law[686]. Section 32 of the Pak makes international offenders liable.[687]

Philippines

Six weeks after the dissemination of the "Love Bug" virus,[688] the Republic of the Philippines adopted the "Electronic Commerce Act" which, among other things, created several new cyber-offenses.[689] The offenses are set out in § 33(a) of the Act, which states that the following "shall be penalized by fine and/or imprisonment":

> Hacking or cracking which refers to unauthorized access into or interference in a computer system/server or information and communication system; or any access in order to corrupt, alter,
> steal, or destroy using a computer or other similar information and communication devices, without the knowledge and consent of the owner of the computer or information and communications system, including the introduction of computer viruses and the like, resulting in the corruption, destruction, alteration, theft or loss of electronic data messages or electronic document shall be punished by a minimum fine of one hundred thousand pesos (P100,000.00) and a maximum commensurate to the damage incurred and a mandatory imprisonment of six (6) months to three (3) years. [690]

Singapore

Singapore's cybercrime legislation appears in the Computer Misuse Act which was adopted in 1998.[691] Part II of the Act created six new offenses: unauthorized access;[692] access with intent to commit or facilitate commission of an offense;[693] unauthorized modification of computer material;[694]

---

[685] *Id.*

[686] *Id.*

[687] *Id.*

[688] *See* § I, *supra.*

[689] Republic of the Philippines, Republic Act No. 8792 - Electronic Commerce Act (June 14, 2000), http://www.mcconnellinternational.com/services/country/philippines.pdf.

[690] *Id.* at Part V - § 33(a).

[691] *See* Singapore, Computer Misuse Act (Cap. 50A, Rev. ed. 1998), http://www.lawnet.com.sg/freeaccess/CMA-Details.htm.

[692] *See id.* at Part II - § 3(1) ("any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both").

[693] *See id.* at Part II - § 4(1) ("Any person who causes a computer to perform any function for the purpose of securing access to any program or data held in any computer with intent to commit an offence to which this section applies shall be guilty of an offence").

unauthorized use or interception of computer service;[695] unauthorized obstruction of use of computer;[696] and unauthorized disclosure of access code.[697] The Computer Misuse Act also criminalizes aiding and abetting and attempting to commit any of these offenses.[698]

South Korea

South Korea has two methods of implementing computer crime laws.[699] They have established numerous articles within their criminal code, which went into effect on July 1, 1996, and they have implemented the Promotion of Utilization of Information and Communications Network Act, which went into effect on July 1, 1999.[700]

Within the criminal code, Article 141-1 criminalizes the destruction of documents of public offices, including electromagnetic records.[701] Article 227-2 makes it a crime to falsify or alter electromagnetic documents of a public official or a public office.[702] Article 232-2 criminalizes

---

[694] *See id*. at Part II - § 5(1) ("any person who does any act which he knows will cause an unauthorised modification of the contents of any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both").

[695] *See id*. at Part II - § 6(1) ("any person who knowingly --
(a) secures access without authority to any computer for the purpose of obtaining, directly or indirectly, any computer service; (b) intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of an electro-magnetic, acoustic, mechanical or other device; or (c) uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence under paragraph (a) or (b), shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both").

[696] *See id*. at Part II - § 7(1) ("Any person who, knowingly and without authority or lawful excuse (a) interferes with, or interrupts or obstructs the lawful use of, a computer; or (b) impedes or prevents access to, or impairs the usefulness or effectiveness of, any program or data stored in a computer, shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both").

[697] *See id*. at Part II - § 8(1) ("Any person who, knowingly and without authority, discloses any password, access code or any other means of gaining access to any program or data held in any computer shall be guilty of an offence if he did so (a) for any wrongful gain; (b) for any unlawful purpose; or (c) knowing that it is likely to cause wrongful loss to any person").

[698] *See id*. at Part II - § 10(1) ("Any person who abets the commission of or who attempts to commit or does any act preparatory to or in furtherance of the commission of any offence under this Act shall be guilty of that offence and shall be liable on conviction to the punishment provided for the offence").

[699] http://icic.sppo.go.kr/english_d_2.htm.

[700] *Id.*

[701] *Id.* at Article 141-1:

> A person who damages or conceals documents or other goods, or special media records, such as electromagnetic records, etc., used by public offices or spoils its utility by other methods, shall be punished by imprisonment for not more than seven years or by a fine not exceeding ten million won.

[702] *Id.* at Article 227-2:

falsification or alteration of private electromagnetic records.[703] Article 314-2 makes it a criminal offense to interfere with business by damaging or destroying any data processors, including computers or electromagnetic records.[704] Article 347-2 make it a crime to commit fraud by the use of a computer.[705] Article 366 makes it a crime to damage, destroy, or conceal another person's property, including electromagnetic records.[706]

Within the Promotion of Utilization of Information and Communications Network Act; Chapter V, Article 19 secures the safety of information, the truthfulness of the information, and protects users against unwanted advertising.[707] Article 20 imposes obligations on providers of information and communications services, forbidding them from committing acts that are harmful to the security of the state, acts detrimental to public safety and moral, injurious to the economic order of the state, hurtful to the development of the economy, and criminal activities.[708] Article 21 restricts the outflow of key

---

> A person with the intention of making any error in management of affairs, falsifies or alters electromagnetic documents of a public official or a public office shall be punished by imprisonment for not more than ten years.

[703] *Id.* at Article 232-2:

> A person who falsifies or alters, with the intention of making any error in management of affairs, any special media records, such as another person's electromagnetic records pertaining to a right, duty, or a certification of fact, shall be punished by imprisonment for not more than five years, or a fine not exceeding ten million won.

[704] *Id.* at Article 314-2:

> A person who interferes with another person's business by damaging or destroying any data processor, such as a computer, or special media records, such as electromagnetic records, or inputting false information or improper order into the data processor, or making any impediment in processing any data by any other way, shall also be subject to the same punishment as referred to in paragraph (1). (Imprisonment for not more than five years or a fine not exceeding fifteen million won.)

[705] *Id.* at Article 347-2:

> A person who acquires any benefits to property or has a third person acquire them, by making any data processed after inputting false information or improper order into the data processor, such as a computer, etc., shall be punished by imprisonment for not more than ten years, or a fine not exceeding twenty million won.

[706] *Id.* at Article 366:

> A person who, by destroying, damaging, or concealing another person's property, document or special media records, such as electromagnetic records, etc., or by any other means, reduces their utility, shall be punished by imprisonment for not more than three years or a fine not exceeding seven million won.

[707] http://icic.sppo.go.kr/english_d_2.htm Article 19:

> (1) The providers of information and communications services shall take measures to secure the safety of the information and communications networks and the trustworthiness of the information that they have.
> (2) The providers of information and communications services and the users of the services shall not transmit advertising information for the purpose of profits against the will of the addressees.
> (3) No person shall infringe on or impair illegally and unfairly the protective measures referred to in paragraph (1).

[708] *Id.* at Article 20:

> In rendering the information and communications services, the providers of information and communications services, the electronic document relaying operators, the persons engaged in those businesses and all the users shall not perform acts falling under each of the following subparagraphs:
> 1. Acts that are harmful to the security of the state;

information, enabling the Minister of Information to take any necessary measures to prevent information leaks to foreign countries.[709] Article 22 makes it a criminal act to damage information of other's, infringe upon the information, steal, or leak the secrets of other persons.[710] Chapter VII; Articles 28 and 29 of the Act provides for penal provisions for violators of the Act.[711]

Taiwan

In 1997, Taiwan amended its Criminal Code to include prohibitions directed at several varieties of cybercrime.[712] The revised Criminal Code does not make simple hacking an offense,[713] but it does

---

2. Acts that are detrimental to public safety and order as well as public morals;
3. Acts that are injurious to the economic order of the state or hurtful to the development of the economy;
4. Criminal activities or other activities that are banned by this act or other acts.

[709] *Id.* at Article 21:

(1) The Minister of Information and Communication may let the providers of information and communications services or the users take measures necessary to prevent key information on the domestic industry, economy, science and technologies from leaking out to foreign countries by means of the information and communications network
(2) Matters concerning the scope of the key information and the contents of measures necessary to protect it under paragraph (1) shall be stipulated by Presidential Decree.

[710] *Id.* at Article 22:

No person shall be permitted to damage the information of other persons, which is processed, stored and transmitted by means of the information and communications network, and to infringe on, steal or leak the secrets of other persons.

[711] *Id.* at Article 28:

A person, who has damaged the personal information and infringed on, stolen or leaked the secrets of other persons in violation of the provisions of Article 22 shall be punished by imprisonment for not more than five years or by a fine not exceeding fifty million won.

Id. at Article 29:

A person, who has infringed on or damaged the protective measures for the information and communications network in violation of the provisions of Article 19(3), shall be punished by imprisonment for not more than three years or by a fine not exceeding thirty million won.

[712] *See* George C.C. Chen, *International Response to Cyber Crime: Asian Perspective*, 1999 Conference on International Cooperation to Combat Cyber Crime and Terrorism – Stanford University, Dec. 6-7, 1999, http://www.oas.org/juridico/english/chen.htm.

[713]

> Taiwan's Criminal Code covers breaking and entering with regard to a dwelling or other structure. . . . A computer hacker might break into a computer system, and although he might not violate any other right or cause any damage therein, the simple act of breaking and entering is a violation of the freedom from interference that these provisions aim to preserve for houses and other physical premises. After considerable debate, it was decided that access to another computer system by itself is not a criminal offence unless any of the above offences are committed.

Id. The "above offences" include forgery, larceny and damage or destruction of property. *Id.*

criminalize the following: disclosure of secrets;[714] offenses against e-mail;[715] causing damage or injury;[716] disrupting the operation of a computer or computer system;[717] computer fraud;[718] computer forgery;[719] and theft.[720]

Vietnam

Vietnam has recently enacted new legislation to prosecute Internet related crimes. Included in the new legislation is Article 41[721] which addresses administrative breaches of regulations, Article 224[722] of

---

[714] *See id.* (Article 318-1: "'A person who without proper reason discloses secrets which learned or obtained through use of a computer or other similar device shall be punished with imprisonment of up to two years, detention or a fine of not more than 5000 yuan'").

[715] *See id.* ("Article 315: 'A person who without proper reason opens or conceals a sealed letter, document or picture belonging to another shall be punished by detention or a fine of not more than 3000 yuan. A person who without proper reason uses another method to gain unauthorized access to any of the foregoing shall be subject to the same punishment'").

[716] *See id.* ("Article 352: 'A person who in a manner likely to cause injury to the public or to another destroys, abandons, or damages a document belonging to another shall be punished with imprisonment of not more than three years, detention, or a fine of not more than 10,000 yuan'").

[717] *See id.* ("Article 352: 'A person who in a manner likely to cause injury to the public or to another interferes with the processing of another's electromagnetic record shall be subject to the same punishment'").

[718] *See id.* ("Article 339-3: 'A person who intentionally and improperly uses false information or an improper method to input into a computer or other similar device to take or cause the loss of property rights, modify a record, or obtain another's property shall be punished by imprisonment ranging from one to seven years'").

[719]The Criminal Code was amended to bring electronic records within the scope of its existing prohibition on forgery. *See id.* ("Article 220: 'A writing, mark, picture or photograph on a paper or a thing which by custom or by special agreement is sufficient evidence of the intention therein contained shall be considered a document within the meaning of this Chapter and other chapters herein. A sound, video or electromagnetic record which by way of a machine or computer expresses a sound, impression or mark which is sufficient evidence of the intention therein contained shall be considered the same as above. Electromagnetic record means an electronic, magnetic, or other method of record which is imperceptible to human senses and is used in operation of a computer'").

[720] The theft provisions of the Criminal Code were amended to encompass theft of intangibles. *See id.* ("Article 323: 'Electric energy, thermal energy, and other forms of energy or electromagnetic record shall be movables within the meaning of this Chapter'").

[721] *Decree No. 55 - Article 41.* Acts of breach, forms and measures of penalty for administrative breaches of regulations relating to the internet shall be as follows:

1. A warning or a fine of fifty thousand (50,000) to two hundred thousand (200,000) Vietnamese dong shall be imposed for an act of failure to make declaration for renewal procedures when the license for provision of internet services is lost or damaged.
2. A fine of two hundred thousand (200,000) to one million (1,000,000) Vietnamese dong for one of the following acts of breach:
   (a) Using the password, encryption code or personal information of another person to access and use internet services illegally;
   (b) Using software tools to access and use internet services illegally.
3. A fine of one million (1,000,000) to five million (5,000,000) Vietnamese dong shall be imposed for one of the following breaches:

(a) Breach of State regulations on standards and quality in the use of internet services;
(b) Breach of State regulations on prices and tariff for the use of internet services;
(c) Breach of State regulations on management of internet resources in the use of internet services;
(d) Breach of State regulations on internet access and connection management in the use of internet services;
(e) Breach of State regulations on coding and decoding of information on the internet in the use of internet services;
(f) Breach of State regulations on safety and security of internet information in the use of internet services.

4. A fine of five million (5,000,000) to ten million (10,000,000) Vietnamese dong shall be imposed for one of the following acts of breach:
   (a) Ceasing of suspending the provision of internet services without notifying internet users thereof in advance, except for cases of force majeure;
   (b) Amending, erasing or changing the contents stated in a license for provision of internet services;
   (c) Using a license for provision of internet services which has expired.
5. A fine of ten million (10,000,000) to twenty million (20,000,000) Vietnamese dong shall be imposed for one of the following breaches:
   (a) Breach of State regulations on standards and quality in the provision of internet services;
(b) Breach of State regulations on prices and tariff for the provision of internet services;
(c) Breach of State regulations on management of internet resources in the provision of internet services;
(d) Breach of State regulations on internet access and connection management in the provision of internet services;
(e) Breach of State regulations on coding and decoding of information on the internet in the provision of internet services;
(f) Breach of State regulations on safety and security of internet information in the provision of internet services;
(g) Using the internet with the intention of threatening, harassing, and defaming the honor and human dignity of other persons, which is not so serious as to require prosecution for criminal liability;
   (h) Loading onto the internet, or abusing the internet to disseminate, debauched images and information, or any other information which is contrary to the law relating to contents of information on the internet, which is not so serious to require prosecution for criminal liability;
(i) Stealing a password, encryption code, or private information of any organization or individual and popularizing its use among others;
(j) Any breach of the regulations on computer operations, exploitation and use, causing chaos, or blocking or deforming or destroying the data on the internet, which is not so serious as to require prosecution for criminal liability.
6. A fine of twenty million (20,000,000) to fifty million (50,000,000) Vietnamese dong shall be imposed for one of the following acts of breach:
   (a) Establishing a system of equipment and providing internet services without complying with the provisions stipulated in the license;
   (b) Creating and deliberately disseminating or spreading virus programs on the internet, which is not so serious as to require prosecution for criminal liability.
7. A fine of fifty million (50,000,000) to seventy million (70,000,000) Vietnamese dong shall be imposed for an act of establishing an equipment system and providing internet services without a license.
8. In addition to administrative penalties, depending on the nature and seriousness of the breach, an organization or individual may be subject to one or more forms of additional penalty or remedial measures as follows:
   (a) Temporary or permanent suspension of provision and use of internet services, in the case of acts of breach referred to in clauses 2(a), 2(b), 3, 5 and 6(b) of article 41;
   (b) Being deprived of the right to use a license for a definite or indefinite period, in the case of breaches referred to in clauses 4(b) and 6(a) of article 41;
   (c) Confiscation of material evidence and means used to commit an administrative breach, in the case of breaches referred to in clauses 4(b), 6(a) and 7 of article 41;
   (d) Request for restitution of changes resulting from an administrative breach, in the case of breaches referred to in clauses 5(j) and 6(b) of article 41.

Seck Yee Chung, International Attorney at Law, Baker & McKenzie, Ho Chi Minh City, Vietnam

the Penal Code which covers the creation, spread and scattering of electronic virus programs, Article 225[723] encompasses breaching regulations on operating, exploiting and using computer networks, and Article 226[724] on illegally using information in computer networks.

---

[722] *Article 224: Creating and spreading, scattering electronic virus programs:*

1. Those who create and intentionally spread or scatter virus programs through computer networks or by other methods, thus causing operation disorder, blockading, deformation or destruction of computer data or who have already been disciplined or administratively sanctioned for this act but continue to commit, shall be subject to a fine of between five million dong (VND5,000,000) and one hundred million dong (VND100,000,000) or a prison term of between six months and three years.
2. Committing the crime and causing very serious or particularly serious consequences, the offenders shall be sentenced to between two and seven years of imprisonment.
3. The offenders may also be subject to a fine of between five million dong (VND5,000,000) and fifty million dong (VND50,000,000), a ban from holding a certain posts, practicing certain occupations or doing certain jobs for one to five years.

Seck Yee Chung, International Attorney at Law, Baker & McKenzie, Ho Chi Minh City, Vietnam

[723] *Article 225: Breaching regulations on operating, exploiting and using computer networks*

1. Those who are allowed to use computer networks but violate the regulations on operating, exploiting and using the computer networks, causing operation disorder, blockading or deformation or destruction of computer data or who have already been disciplined, administratively sanctioned for such act but continue to commit it, shall be subject to a fine of between five million dong (VND5,000,000) and one hundred million dong (VND100,000,000), non-custodial reform for up to three years or a prison term of between one and three years.
2. Committing the crime in one of the following circumstances, the offenders shall be sentenced between two and five years of imprisonment:
   a. In an organized manner;
   b. Causing very serious or particularly serious consequences.
3. The offenders may also be subject to a fine of between five million dong (VND5,000,000) and fifty million dong (VND50,000,000), a ban from holding certain posts, practicing certain occupations or doing certain jobs for one to five years.

Seck Yee Chung, International Attorney at Law, Baker & McKenzie, Ho Chi Minh City, Vietnam

[724] *Article 226: Illegally using information in computer networks*

1. Those who illegally use information in computer networks and computers as well as put information into computer networks in contravention of law provisions, causing serious consequences, who have already been disciplined, administratively sanctioned but continue to commit it, shall be subject to a fine of between five million dong (VND5,000,000) and fifty million dong (VND50,000,000), non-custodial reform for up to three years or a prison term of between six months and three years.
2. Committing the crime in one of the following circumstances, the offenders shall be sentenced to between two and five years of imprisonment:
   a. In an organized manner;
   b. Causing very serious or particularly serious consequences.
4. The offenders may also be subject to a fine of between three million dong (VND3,000,000) and thirty million dong (VND30,000,000), a ban from holding certain posts, practicing certain occupations or doing certain jobs for one to five years.

Seck Yee Chung, International Attorney at Law, Baker & McKenzie, Ho Chi Minh City, Vietnam

VI. NORTH AFRICA AND THE MIDDLE EAST

Egypt

A study published in December of 2000 found that Egypt had no cybercrime specific laws in place. [725]

Iran

A study published in December of 2000 found that Iran had no cybercrime specific laws in place. [726] It noted that "for the past six years Iran has examined various aspects of cyber law," including "computer offenses", but so far no laws have been adopted.[727] In June of 2001, the Iran Telecommunications Company issued regulations "to filter all materials presumed immoral or contrary to state security, including the Web sites of opposition groups," and to bar Internet access for those under eighteen.[728]

Israel

Israel's cybercrime legislation appears in its Computers Law, 5755, which has been in effect since 1995.[729] The Computers Law creates the following offenses: disrupting or interfering with the operation of a computer; [730] disseminating "specious information" or "specious output"; [731] unauthorized

---

[725] *See Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information, supra* note 1.

[726] *Id*.

[727] *Id.*

[728] *Iran Takes Tough Measures to Stop Internet Use*, REUTERS, June 24, 2001, http://dailynews.yahoo.com/h/nm/20010624/wr/iran_access_dc_1.html.

[729] *See* Israel, Computers Law, 5755-1995, http://www.law.co.il/computer-law/main.htm.

[730] *See id*. at Chapter B § 2:

> A person who unlawfully perpetrates one of these is liable to imprisonment for a period of three years:
>
> (1) Disrupts the normal operation of a computer or interferes with the use thereof;
> (2) Deletes computer material, causes a change therein, muddles it in any other way or interferes with the use thereof.

[731] *See id*. at Chapter B § 3:

> (a) A person who perpetrates one of these is liable to imprisonment for a period of five years:
>
> (1) Transfers to another or stores in a computer specious information or commits an action concerning information in such a way that the consequence is specious information or specious output;
> (2) Writes software, transfers software to another, or stores software in a computer in such a way that the consequence of the use thereof is specious information or specious output, or operates a computer using said software.

access; [732] unauthorized access to commit another offense; [733] and disseminating viruses or other harmful programs.[734]

Jordan

A study published in December of 2000 found that Zimbabwe had no cybercrime specific laws in place. [735] Subscribers to Internet services are explicitly required to abide by the laws applicable in Jordan, especially pertaining to publications, limitations on opinions expressed, and all the relevant Jordanian laws.[736]

Kazakhstan

A study published in December of 2000 found that while Kazakhstan currently had no cybercrime specific laws in place, "state bodies" were "developing a law regarding cyber offenses." [737]

Lebanon

Lebanon has yet to enact specific cyber crime legislation. However, through funds from the World Bank, Lebanon has drafted the National Information Technology Policy and Strategy document.[738]

> (b) In this section, "specious information" and "specious output" - information or output that has the ability to mislead, pursuant to the objectives of the use thereof.

[732] *See id*. at Chapter B § 4 ("A person who unlawfully penetrates computer material located in a computer is liable to imprisonment for a period of three years; for the purpose of this matter, "penetration of computer material" - penetration by means of communication with or connection to a computer, or by the operation thereof, but excluding penetrating computer material that is eavesdropping under the Eavesdropping Law, 5739-1979").

[733] *See id*. at Chapter B § 5 ("Any person who does something forbidden under Section 4 in order to commit an offense under any law, with the exception of under this law, is liable to imprisonment for a period of five years").

[734] *See id*. at Chapter B § 6:

> (a) A person who writes a software program in such a manner that it is capable of causing damage or disruption to an unspecified computer or computer material in order to cause unlawful damage or disruption to a computer or computer material, specified or unspecified, is liable to imprisonment for a period of three years.
> (b) A person who conveys to another, or who infiltrates another's computer with, a software program that is capable of causing damage or disruption as stipulated in Subsection (a), in order to cause unlawful damage or disruption as aforesaid, is liable to imprisonment for a period of five years.

[735] *See id.*

[736] "Terms and Conditions" related to the services of the National Equipment and Technical Services Company of Jordan, NETS, *at* http://www.nets.com.jo/FAQs/terms.html.

[737] *See id*.

[738] http://www.omsar.gov.lb/english/epolicy.html#b.

The approach of this policy is for the government to take responsibility for key regulatory functions including privacy, intellectual property, security, and information content.[739]

Morocco

A study published in December of 2000 found that Morocco currently had no cybercrime specific laws in place, but that an "inter-ministerial commission sponsored by the Prime Minister" was "working on security issues."[740]

Oman

Rules and regulations of an ISP entitled GTO prohibit unauthorized or unlawful gaining or trying to gain access to any computer systems or networks through the use of the ISP services and any unlawful activities which are contrary to the social, cultural, political, religious or economical values of the Sultanate of Oman. Customers are also warned that any abuse and misuse of the Internet services through email or news or by any other means, including posting or soliciting obscene materials, hacking or trying to hack, shall result in criminal or civil lawsuits against the perpetrators. The ISPs also reserves the right to disconnect the service without notice.

Saudi Arabia

All communications are routed through a state proxy-server, which blocks access to sites deemed unacceptable for religious, moral, national security, or other reasons set out by the state.[741]

Sudan

A study published in December of 2000 found that Sudan had no cybercrime specific laws in place.[742] Sudan plans to "invite lawyers, legislators and computer professionals to a workshop" where the discussion will focus on the drafting of cybercrime legislation.[743]

Syria

President Bashar al-Assad has pledged to take Syria into the computer age and Internet access is now available in the country.[744]

Tunisia

---

[739] *Id.*

[740] *See Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information*, *supra* note 1.

[741] David Hirst, "Saudi Arabia Lets Internet Blossom, But With Controls," *St. Petersburg Times*, July 20, 1999, Pt. 14A.

[742] *See Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information*, *supra* note 1.

[743] *Id.*

[744] *Internet in Syria – August 3, 2000 Syria Begins Internet Expansion,"* Café-Syria, http://www.café-syria.com/Internet.htm.

Tunisia has not enacted any specific cyber crime legislation.[745]

Turkey

Turkey's Criminal Code defines several types of cybercrime, to wit:

Article 525/a - (Annexed by Code 3756 Art. 21, 06.06.1991)

Whoever obtains programs or data or another component from an automatic data processing system illegally, shall be punished by imprisonment for one year to three years and a heavy fine of 1,000,000 to 15,000,000 liras.

Whoever uses, transfers or copies programs, data or another component in anautomatic data processing system, with the purpose of harming anybody, shall suffer the punishment in the above mentioned paragraph.

Article 525/b - (Annexed by Code 3756 Art. 22, 06.06.1991)

Whoever destroys or changes or deletes or prevents from operating or ensures incorrectly operating an automatic data processing system or data or another component, completely or partially, for the purpose of harming anyone or deriving a benefit for himself or anybody else, shall be punished by imprisonment for two years to six years and a heavy fine of 5,000,000 to 50,000,000 liras.

Whoever derives a legal benefit for himself or anybody else, using an automatic data processing system, shall be punished by imprisonment for one year to five years and a heavy fine of 2,000,000 to 20,000,000 liras.

Article 525/c - (Annexed by Code 3756 Art. 23, 06.06.1991

Whoever puts data or other components into an automatic data processing system or alters existing data or other components, in order to generate a counterfeit document for the purpose of using as evidence in jurisprudence, shall be punished by imprisonment for one year to three years. Whoever uses knowingly the abovementioned-altered one shall be punished by imprisonment for six months year to two years.[746]

United Arab Emirates

There currently is no cybercrime legislation in the United Arab Emirates, though a draft cybercrime law is in process.[747] Etisalat, the Emirates Telecommunications Corporation, has promulgated

---

[745] http://www.mossbyrett.of.no/info/legal.html.

[746] McConnell International, *Cyber Security Legislation*, http://www.mcconnellinternational.com/services/Updatedlaws.htm.

[747] *See, e.g.,* Aftab Kazmi, *UAE "Needs Task Force to Fight Cyber Crime,"* GULF NEWS, June 4, 2001, http://www.gulf-news.com/Articles/news.asp?ArticleID=18865 (UAE General Information Authority had "submitted a list of cyber crimes and a report to the Ministry of Justice which has set up a committee to draft laws and regulations" dealing with cybercrime). *See also* Greg Wilson, *Ashurst Case Sparks E-Legalisation Debate*, WWW.ITP.NET, http://www.itp.net/features/98327661040647.htm; Jihad Abdullah, *Was Arab ISP Hack Illegal?*, WIRED NEWS, July 5, 2000, http://www.wired.com/news/infostructure/0,1377,37401,00.html.

"terms and conditions" for the use of its services and an "acceptable use policy",; it reserves the right to initiate "such criminal or civil proceedings" as it deems necessary to secure the enforcement of these regulations.[748]

VII. SUB-SAHARAN AFRICA

Gambia

A study published in December of 2000 found that Gambia currently had no cybercrime specific laws in place.[749] Gambia is "planning a national information technology initiative" which might produce such legislation," although the capacity for drawing up a legal framework is limited."[750]

Kenya

Kenya has not enacted any specific cyber crime legislation.[751]

Lesotho

A study published in December of 2000 found that Lesotho, too, currently had no cybercrime specific laws in place.[752] It has established "special interest groups to look at the various aspects of information security relating to e-commerce.[753]

Nigeria

A study published in December of 2000 found that Nigeria had no cybercrime specific laws in place.[754]

South Africa

A study published in December of 2000 found that South Africa had no cybercrime specific laws in place.[755]

---

[748] *See* Terms & Conditions, ETISALAT, http://www.emirates.net.ae/terms.html#2.

[749] *See Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information*, *supra* note 1.

[750] *Id.*

[751] Email correspondence between attorney in Kenya and Adam Savino, student at the University of Dayton School of Law (May, 2002) (on file with authors).

[752] *See Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information*, *supra* note 1.

[753] *Id*.

[754] *Id*.

[755] *Id.*

Zambia

A study published in December of 2000 found that Zambia currently had no cybercrime specific laws in place.[756] It also noted that Zambian officials had prepared a draft Telecommunications and Information Technology Council Act.[757]

Zimbabwe

A study published in December of 2000 found that Zimbabwe had no cybercrime specific laws in place.[758]

VIII. AUSTRALIA, NEW ZEALAND AND THE PACIFIC ISLANDS

Australia

Australia's Crimes Act 1914 establishes four cyber-offenses:[759] unlawful access to data in Commonwealth and other computers;[760] damaging data in Commonwealth and other computers;[761]

---

[756] See *id.*

[757] *See id*. *See also* Republic of Zambia, Draft Legislation – The Telecommunications and Information Technology Council Act, http://www.mcconnellinternational.com/services/country/zambia.pdf.

[758] *See Cyber Crime . . . and Punishment? Archaic Laws Threaten Global* Information, *supra* note 1.

[759] *See* Australia, Crimes Act 1914, Part VIA, http://scaleplus.law.gov.au/.

[760] *See id*. at § 76B:

> (1) A person who intentionally and without authority obtains access to:
> (a) data stored in a Commonwealth computer; or
> (b) data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer;
> is guilty of an offence. Penalty: Imprisonment for 6 months.
>
> (2) A person who:
> (a) with intent to defraud any person and without authority obtains access to data stored in a Commonwealth computer, or to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer; or
> (b) intentionally and without authority obtains access to data stored in a Commonwealth computer, or to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer, being data that the person knows or ought reasonably to know relates to:
> (i) the security, defence or international relations of Australia;
> (ii) the existence or identity of a confidential source of information relating to the enforcement of a criminal law of the Commonwealth or of a State or Territory;
> (iii) the enforcement of a law of the Commonwealth or of a State or Territory;
> (iv) the protection of public safety;
> (v) the personal affairs of any person;
> (vi) trade secrets;
> (vii) records of a financial institution; or
> (viii) commercial information the disclosure of which could cause advantage or disadvantage to any person; is guilty of an offence.

unlawful access to data in Commonwealth and other computers by means of Commonwealth facility; [762] and damaging data in Commonwealth and other computers by means of Commonwealth facility.[763]

Fiji Islands

The Fiji Islands have not enacted any specific cyber crime legislation.[764]

New Zealand

A study published in December of 2000 found that New Zealand currently had no cybercrime specific laws in place. [765] It noted that New Zealand was drafting a Crimes Amendment Bill (No. 6) which would address cybercrime. [766]

Penalty: Imprisonment for 2 years.

(3) A person who:
(a) has intentionally and without authority obtained access to data stored in a Commonwealth computer, or to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer;
(b) after examining part of that data, knows or ought reasonably to know that the part of the data which the person examined relates wholly or partly to any of the matters referred to in paragraph (2)(b); and
(c) continues to examine that data; is guilty of an offence.
Penalty: Imprisonment for 2 years.

(4) For the purposes of an offence against subsection (1), (2) or (3), absolute liability applies to whichever one of the following physical elements of circumstance is relevant to the offence:
(a) that the computer is a Commonwealth computer;
(b) that the computer is not a Commonwealth computer.

[761] *See id*. at Part VIA § 76C:

(1) A person who intentionally and without authority:
(a) destroys, erases or alters data stored in, or inserts data into, a Commonwealth computer;
(b) interferes with, or interrupts or obstructs the lawful use of, a Commonwealth computer;
(c) destroys, erases, alters or adds to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer; or
(d) impedes or prevents access to, or impairs the usefulness or effectiveness of, data stored in a Commonwealth computer or data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer;
is guilty of an offence. Penalty: Imprisonment for 10 years.

(2) For the purposes of an offence against subsection (1), absolute liability applies to whichever one of the following physical elements of circumstance is relevant to the offence:
(a) that the computer is a Commonwealth computer;
(b) that the computer is not a Commonwealth computer.

[762] *See id*. at Part VIA § 76D.

[763] *See id*. at Part VIA § 76E.

[764] University of the West Indies Law Library, Cave Hill Campus, St. Michael, Barbados.

[765] *See Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information*, *supra* note 1.

[766] *Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information*, *supra* note 1. *See also* Crimes Amendment Bill (No. 6) – Submission from the Internet Society of New Zealand, Feb. 9, 2001, http://www.isocnz.org.nz/issues/iswg010209submsm_crimes-amend-bill-6.html.